Administrator's Manual

310HD / 320HD / 420HD IP Phones

Version 2.0.0

AudioCodes

HD VoIP
Sounds Better

Table of Contents

List of Figures

List of Tables

<div style="border:1px solid blue; padding:10px">

Notice

This manual shows administrators how to set up and configure AudioCodes' 310HD, 320HD and 420HD IP Phones.

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document and other documents can be viewed by registered customers at http://www.audiocodes.com/downloads.

© Copyright 2012 AudioCodes Ltd. All rights reserved.
This document is subject to change without notice.

Date Published: Oct-16-2012

</div>

Trademarks

AudioCodes, AC, AudioCoded, Ardito, CTI2, CTI², CTI Squared, HD VoIP, HD VoIP Sounds Better, InTouch, IPmedia, Mediant, MediaPack, NetCoder, Netrake, Nuera, Open Solutions Network, OSN, Stretto, TrunkPack, VMAS, VoicePacketizer, VoIPerfect, VoIPerfectHD, What's Inside Matters, Your Gateway To VoIP and 3GX are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners.

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and service are provided by AudioCodes' Distributors, Partners, and Resellers from whom the product was purchased. For Customer Support for products purchased directly from AudioCodes, contact support@audiocodes.com.

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used.

Related Documentation

Document Name
300HD IP Phone Series Release Notes
310HD IP Phone Quick Guide
310HD IP Phone User's Manual
320HD IP Phone Quick Guide
320HD IP Phone User's Manual
420HD IP Phone User's Manual
420HD IP Phone Quick Guide

Regulatory Information

Compliancy and Regulatory Information can be viewed at   :
http://www.audiocodes.com/library.

> **Note:** Throughout this document, where features can be configured using the Web interface or Configuration File, the Web parameter is displayed in the regular font above its corresponding Configuration File parameter, which is enclosed in square brackets in bold font type.

1   Introduction

This manual is intended for the system administrator responsible for setting up and configuring the 310HD, 320HD and 420HD IP Phones.

AudioCodes' IP phones are based on AudioCodes' proprietary High Definition (HD) voice technology, providing clarity and a rich audio experience in Voice-over-IP (VoIP) calls. The phones are fully-featured telephones that provide voice communication over an IP network, allowing you to place and receive phone calls, put calls on hold, transfer calls, make conference calls, and so on.

The phone offers a wide variety of management and configuration tools:

- **Phone's LCD display user interface -** easy-to-use, menu-driven display screen, providing basic phone configuration and status capabilities

- **Web interface -** provides a user-friendly Web interface that runs on a Web browser (Microsoft® Internet Explorer is the recommended browser).

- **Configuration file -** text-based file (created using any plain text editor such as Microsoft's Notepad) containing configuration parameters and which is loaded to the phone using the Web interface or a TFTP, FTP, HTTP or HTTPS server.

- **TR-069** for remote configuration and management

- **CLI over Telnet**

For a detailed description on hardware installation and for operating the phone's call features, refer to the *User's Manual*.

Reader's Notes

Part I

Configuration Tools

Reader's Notes

2   IP Phone User Interface

The IP phone provides a Liquid Crystal Display (LCD) based screen, offering an intuitive, menu-driven interface for configuring the phone. The administrative tasks are performed in the phone's **Administration** menu.

2.1   Accessing the Administration Menu

The procedures to access the **Administration** menu using the 310HD, 320HD and 420HD IP Phones, are described below.

> **Notes:**
>
> - The default password is 1234. To change the login password, use the phone's Web interface or Configuration file.
> - Once you have entered the password, the access session is applied to all the submenus.
> - To change the **Administration** menu's login password, use the

2.1.1   310HD IP Phone

The submenus of the **Administration** menu are password protected. When attempting to access a submenu, the phone prompts you to enter the access password.

➢ **To access the Administration menu:**

1. In idle display, press the MENU key, and then select the **Administration** menu (using the ▲ and ▼ Navigation keys),

```
Status
Administration
```
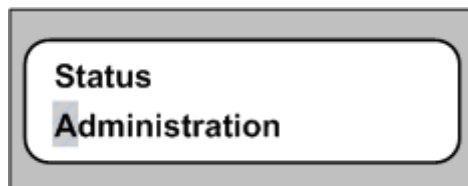
2. Press the ENTER key; you are prompted for a password:

```
Enter Password
```

3. Enter the password, and then press the ENTER key; the **Administration** submenus are displayed.

2.1.2 320HD IP Phone

The **Administration** menu is password protected. The default password is "1234".

➢ **To access the Administration menu:**

1. In idle display, press the MENU key; the Menu list is displayed:

```
Menu                    04:00
 3. Speed Dial            ▲
 4. Settings
 5. Status
 6. Administration
Select                  Back
```
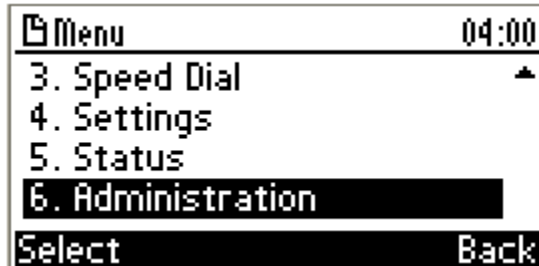
2. Using the ▲ and ▼ Navigation keys, choose the **Administration** submenu, and then press the **Select** softkey; you are prompted for a password:
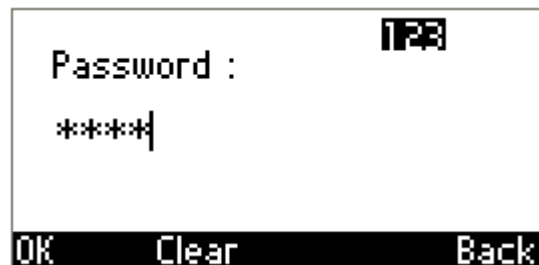
```
                        123
 Password :

 ****|


OK    Clear        Back
```

3. Enter your password, and then choose **OK**. When entering the password, you can change between numerals and letters, by pressing the pound (#).

2.1.3   420HD IP Phone

Accessing the **Administration** menu of the 420HD IP phone is identical to accessing that of the 320HD IP phone. The phone is password protected. The default password is "1234".

➢ **To access the Administration menu:**

1.   In idle display, press the MENU key; the Menu list is displayed. Press the navigation control's lower rim to navigate to the **Administration** option.
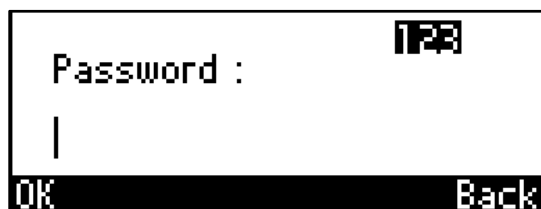
```
Menu
 5. Status
 6. Administration
Select                    Back
```

2.   Press the **Select** softkey; you are prompted for a password.

```
                    123
Password :

|
OK                        Back
```

3.   Enter your password, and then choose **OK**. When entering the password, you can change between numerals and letters by pressing pound (#).

```
                    123
Password :

****|
OK     Clear          Back
```
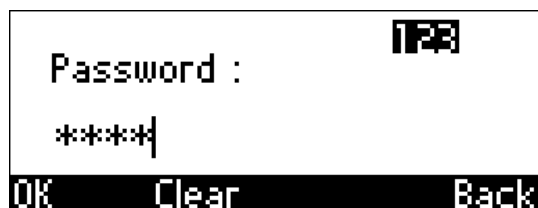
2.2 Changing Display Language

This section describes how to change the language of the LCD display of the IP Phones.

2.2.1 310HD IP Phone
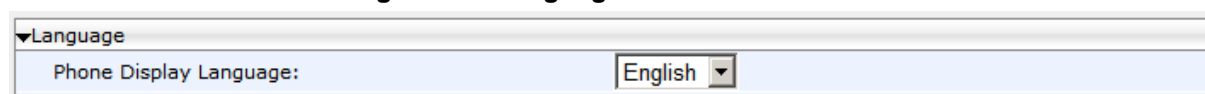
The Changing Display Language feature can be configured using the Web or Configuration File, as described below.

➢ **To choose a language:**

■ **Using the Web:**

1. Access the 'Language' page (**Configuration** tab > **Personal Settings** menu > **Language**).

Figure 2-1: Language Web Field – 310HD

2. Select the language according to the parameter in the table below, and then click **Submit**; the phone reboots and changes the LCD display language accordingly.

■ **Using the Configuration File:**

Table 2-1: LCD Display Parameters

Parameter	Description
Phone Display Language **[personal_settings/language]**	Determines the LCD display user interface language. ▪ **[English]** English (default) ▪ **[Spanish]** Spanish ▪ **[Italian]** Italian ▪ **[Portuguese]** Portuguese ▪ **[German]** German ▪ **[Russian]** Russian ▪ **[Ukraine]** Ukraine ▪ **[Polish]** Polish ▪ **[French]** French
[/system/activation_keys/portuguese_language]	Activation key (string) required to unlock Portuguese language support.
[personal_settings/max_directory_size]	Determines the maximum directory size. The valid range is 0 to 700. The default value is 700. **Note**: To reduce the memory consumption of the phone and to increase performance, this value should be optimized and set to the lowest value according to the actual corporate directory size.

2.2.2   320HD IP Phone
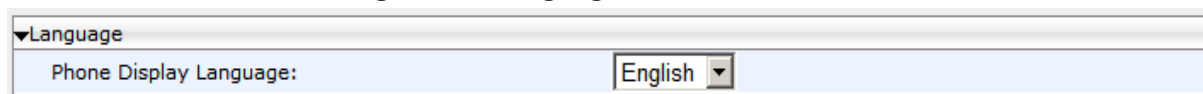
The Changing Display Language feature can be configured using the Web or Configuration File, as described below.

➢ **To choose a language:**

■ **Using the Web:**

1. Access the 'Language' page (**Configuration** tab > **Personal Settings** menu > **Language**).

Figure 2-2: Language Web Field – 320HD

▼Language	
Phone Display Language:	English ▼

2. Select the language according to the parameter in the table below, and then click **Submit**; the phone reboots and changes the LCD display language accordingly.

Table 2-2: Language Display Parameters

Parameter	Description
Phone Display Language **[personal_settings/language]**	Determines the LCD display user interface language. ▪ **[English]** English (default) ▪ **[Spanish]** Spanish ▪ **[Russian]** Russian ▪ **[German]** German ▪ **[Ukraine]** Ukraine ▪ **[French]** French ▪ **[Italian]** Italian ▪ **[Hebrew]** Hebrew ▪ **[Polish]** Polish
[personal_settings/lcd_contrast]	Determines the LCD contrast. The valid range is 0 to 14. The default value depends on the actual hardware revision.

Note: **Portuguese** is supported even though it may not be listed in the LCD. To activate Portuguese, contact your AudioCodes representative.

2.2.3   420HD IP Phone
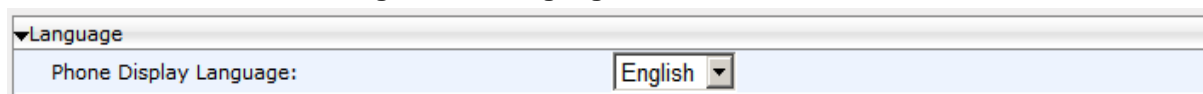
The Changing Display Language feature can be configured using the Web or Configuration File, as described below.

➢ **To choose a language:**

■ **Using the Web:**

1. Access the 'Language' page (**Configuration** tab > **Personal Settings** menu > **Language**).

Figure 2-3: Language Web Field – 420HD

2. Select the language according to the parameter in the table below, and then click **Submit**; the phone reboots and changes the LCD display language accordingly.

Table 2-3: Language Display Parameters

Parameter	Description
Phone Display Language **[personal_settings/language]**	Determines the LCD display user interface language. ▪ **[English]** English (default) ▪ **[Spanish]** Spanish ▪ **[Russian]** Russian ▪ **[German]** German ▪ **[Ukraine]** Ukraine ▪ **[French]** French ▪ **[Italian]** Italian ▪ **[Hebrew]** Hebrew ▪ **[Polish]** Polish
[personal_settings/lcd_contrast]	Determines the LCD contrast. The valid range is 0 to 63. The default value depends on the actual hardware revision.

Note: **Portuguese** is supported even though it may not be listed in the LCD. To activate Portuguese, contact your AudioCodes representative.

3 Web Interface

This chapter describes the phone's embedded Web server interface that is used for configuring the phone.

3.1 Accessing Web Interface

You can use any standard Web browser (such as Microsoft Internet Explorer) to access the phone's Web interface. The IP address used for accessing the Web interface is the phone's IP address, received from a DHCP server or manually configured (static IP address).

➢ **To access the phone's Web interface:**

1. Connect the LAN port of your phone to the IP network (using the Cable or ADSL modem from your Internet Service Provider).

2. Determine the phone's IP address obtained from the DHCP server, using the phone's LCD screen as described in Section 35 on page 219 (in the 'IP Address' field).

3. Open a Web browser, and then in the URL address field, enter the phone's IP address (for example, http://192.168.1.2 or https://192.168.1.2), as displayed below:

The Web login window appears:

Figure 3-1: Web Login Window

4. Alternatively, if your DHCP and DNS servers are synchronized you can access the phone Web browser by using the following method:

http://310hd-<MAC Address>.<Domain Name>

(e.g. http://310hd-001122334455.corp.YourCompany.com)

5. Enter the **User name** and **Password**, and then click **OK**.

> **Note:** The administrator's default login user name and password are "admin"

3.2   Getting Started with the Web

The areas of the Web interface are shown below:

Figure 3-2: Web Interface Areas
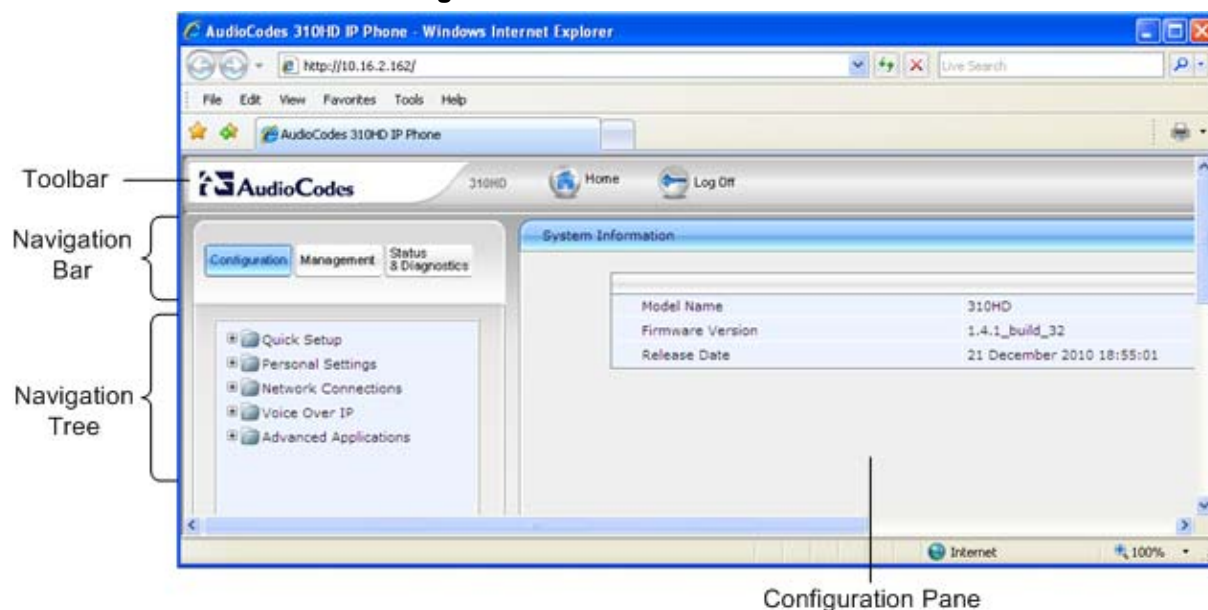
The Web interface is composed of the following main areas:

■ **Toolbar:** displays AudioCodes logo and provides the following buttons:

- 🏠 **Home:** opens the Home page

- 🔑 **Log off:** closes the Web interface

■ **Navigation bar:** provides tabs for accessing the configuration menus:

- **Configuration:** provides menus for configuring the phone.
- **Management:** provides menus for various management tasks such as firmware upgrade and changing the login username and password.
- **Status & Diagnostics:** provides menus for displaying information on the status of the phone, such as call history.

■ **Navigation tree:** tree-like, hierarchical structure of menus pertaining to the selected tab on the Navigation bar.

■ **Configuration pane:** displays the configuration parameters pertaining to a selected menu in the Navigation tree.

4   Configuration File

This section describes the Configuration file and the parameters that you can set in the Configuration file.

4.1   Introduction

The Configuration file can be loaded to the phone using the automatic provisioning mechanism, or manually from your local computer using the Web interface (see Section 3 on page 25). The subsections below describe the Configuration file syntax and linking additional Configuration files to a Configuration file.

4.2   File Syntax

The Configuration file can be created using a standard ASCII, text-based program such as Notepad. The Configuration file is a *.cfg* file with the file name being the phone's MAC address: **<phone's MAC address>.cfg**.

The syntax of the Configuration file is as follows:

```
<parameter name>=<value>
```

Ensure that the Configuration file adheres to the following guidelines:

- No spaces on either side of the equals (=) sign.
- Each parameter must be on a new line.

Below is an example of part of a Configuration file:

```
system/type=310HD
voip/line/0/enabled=1
voip/line/0/id=1234
voip/line/0/description=310HD
voip/line/0/auth_name=1234
voip/line/0/auth_password=4321
```

4.3   Linking Multiple Files

The Configuration file allows you to include links (URL and/or file name) to other Configuration files that provide additional parameter settings. This is especially useful in deployments with multiple phones, where the phones share common configuration but where each phone has some unique settings. In such a scenario, a phone's Configuration file can include unique parameter settings as well as links to additional Configuration files with settings common to all phones.

Linking additional files is achieved by using the **include** function in the phone's Configuration file. For example, the below Configuration file provides links to additional Configuration files (shown in bolded font):

```
system/type=310HD
include 310HD_<MAC>_voip.cfg
include vlan_conf.cfg
include network_conf.cfg
include provisioning_conf.cfg
```

In addition, the Configuration file can provide URL paths (FTP, TFTP, HTTP, or HTTPS) to where the additional files are located, as shown in the example below (shown in bolded font):

```
system/type=310HD
include http://10.10.10.10/310HD_<MAC>_voip.cfg
include https://remote-pc/vlan_conf.cfg
include tftp://10.10.10.10/310HD_<MAC>_network.cfg
include ftp://remote-pc/provisining_conf.cfg
```

> **Note:** If no URL is provided in the Configuration file, the files are retrieved according to the provisioning information (e.g. DHCP Option 160 or 66/67).

4.4   Downloading Configuration File from IP Phone

For more information, see 'Part VIII, Maintenance Section'.

4.5   Creating Configuration Files using VoIProvision Utility

4.5.1   Introduction

When installing AudioCodes' 300HD IP Phones, the integrator or IT manager typically wishes to configure each installed IP phone automatically. Using DHCP options or other methods, the IP phone can be instructed to download a configuration file. This file is typically unique to each IP phone, based on the MAC address. This MAC-specific configuration file is generated with IP phone specific configuration parameters; such as, the extension ID, name and authentication password.

Not all of the iPBX and SoftSwitch vendors (and especially the full solution vendors) include provisioning in their interoperability programs. Therefore, AudioCodes, as an IP Phone vendor, is required to provide a standalone provisioning tool that will enable the provisioning of our phones in such environments.

AudioCodes now provides a tool that assists in the automatic generation of such configuration files. These files can be generated for the initial configuration of the IP phones and then later regenerated for subsequent configuration updates as desired.

4.5.2   Configuration File Format

The detailed format of the 300HD configuration files are described in section 'Configuration File Parameters' in the Administrator's Manual (LTRT-08107 320HD IP Phone Administrator's Manual v1.4.0.pdf and LTRT-09905 310HD IP Phone Administrator's Manual v1.4.pdf).

The following is an output example of an automatically generated MAC-specific file:

```
system/type=310HD
voip/line/0/enabled=1
voip/line/0/id=56832432
voip/line/0/auth_name=3423fdwer2tre
voip/line/0/auth_password=123456
include global.cfg
```

4.5.3   Global Configuration File

In addition to the MAC-specific files, it is recommended to maintain a single global configuration file, which contains parameters that are common to all IP phones in the specific site. The MAC-specific files can call the global file (using the 'include' method) as illustrated in the above example. For more information, see 'Linking Additional Files using "Include" ' in the Administrator's Manual.

4.5.4   VoIProvision Utility Overview

The VoIProvision utility is a generic tool that automatically generates multiple MAC-specific configuration files (*.cfg*). The utility generates a separate *.cfg* file for each IP phone.

In order to execute the utility, the user needs to prepare a *csv* file and a *template* file. The *csv* file contains the tagged records for each IP phone and the template file maps these tagged records to a configuration file format, which can be read by the 300HD IP Phone.

4.5.5 CSV File

The *csv* file contains a list of tags and a list of the tag's values. The first line in the file contains the list of tags (comma-separated) and each of the other lines contains a list of values, where each line record represents an individual IP phone.

The *csv* file is usually exported from the customer's IP-PBX or some other database and typically contains the list of IP phones (e.g. MAC, extension ID, user name and password of each IP phone).

Table 4-1: Example of CSV File

[mac]	[name]	[id]	[password]
00908F123456	Jonathan	4071	12345
00908F123457	David	4418	12345

When opened as a text file, the *csv* file appears similar to the example below:

```
[mac],[name],[id],[password]
00908F123456,Jonathan,4071,12345
00908F123457,David,4418,12345
```

4.5.6 Template File

The template file defines the format of the generated configuration files, but contains tags instead of actual values. The **VoIProvision** utility reads the template file and replaces each tag with actual values from the *csv* file.

Example of a template file:

```
system/type=310HD
voip/line/0/enabled=1
voip/line/0/id=[id]
voip/line/0/auth_name=[name]
voip/line/0/auth_password=[password]
include global.cfg
```

4.5.7 Generated Configuration Files

The generated configuration (*.cfg*) files use a similar format to the template file; however the tags are replaced with the actual values that are read by the VoIProvision utility from the *csv* file. One of the tags defined in the *csv* file, should be used as the *.cfg* file name (in order for the VoIProvision utility to generate a separate *.cfg* file for each line record in the csv file). Typically the tag which defines the MAC address is used as the *.cfg* file name.

4.5.8 Starting the VoIProvision Utility

The VoIProvision utility can run on both the Linux and Windows platforms. The VoIProvision utility initially parses the *csv* file to generate the list of tags. The VoIProvision then reads each line record of values in the *csv* file and for each line record, does the following:

■ Parses the line record to create a list of values

■ Opens the template file

■ Generates the *.cfg* file name and create a new *.cfg* file

■ Reads the template file, associates the mapped tags with actual values from the *csv* file and writes the result to the *.cfg* file

■ Closes the *.cfg* file and template file

4.5.9   Usage

```
USAGE: VoIProvision <csv file> <template file> <.cfg file>
```

Note the following:

- The first line of the *csv* file contains the list of tags (e.g., [mac],[name],[id]).
- The remainder of the *csv* file contains a line record per .cfg file (e.g. 00908f112233,4071,Eitan).
- There is no restriction on the format of the tags (e.g., [tag] or @tag@).
- The template file defines the *.cfg* file format. During VoIProvision run-time, the mapped tags in the template file are associated to actual values that are read from the *csv* file.
- Currently only a single tag can be defined per line record in the template file.
- The *.cfg* file name should represent the string of one of the predefined tags in order to generate a separate *.cfg* file per *csv* line record (e.g. "[mac].cfg").

Reader's Notes

5   TR-069 Management

To connect to the remote management server, the phone's embedded TR-069 client must be configured. The TR-069 Management feature can be configured using the Web or Configuration File, as described below

➢ **To configure TR-069:**

■ **Using the Web:**

   1. Access the 'TR-069' page (**Management** tab > **Remote Management** menu > **TR-069**).

Figure 5-1: TR-069 Web Fields

▼TR-069	
Activate:	Enable
Activation Key:	
ACS URL:	
User:	
Password:	
Request Connection User:	
Request Connection Password:	
Periodic Inform:	Enable
Periodic Inform Interval:	3600

   2. Configure TR-069 according to the parameters in the table below, and then click **Submit**.

■ **Via Configuration File:**

Table 5-1: TR-069 Management Parameters

Parameter	Description
Note: To add a value to these parameters, enter **management/** followed by the parameter name, equal sign and then the value (e.g. `management/tr069/enabled=0`).	
Activate **[management/tr069/enabled]**	Enables TR-069. ▪ **[0]** Disable (default) ▪ **[1]** Enable **Note**: This feature can be enabled only if the valid key is provided in the **feature_key** field.
Activation Key **[management/tr069/activation_key]**	Activation key to enable TR-069 management.
ACS URL **[management/tr069/acs_url]**	URL for connecting the device to the ACS. **Note:** This parameter must be in the form of a valid HTTP or HTTPS URL.
User **[management/tr069/user_name]**	Username used to authenticate the device when making a connection to the ACS.
Password **[management/tr069/password]**	Password used to authenticate the device when making a connection to the ACS.
Request Connection User **[management/tr069/connection_request/ user_name]**	Username to authenticate an ACS making a Connection Request to the device.
Request Connection Password **[management/tr069/connection_request/ password]**	Password to authenticate an ACS making a Connection Request to the device.
Periodic Inform **[management/tr069/inform/enabled]**	Determines whether or not the device must periodically send device information to the ACS using the **Inform method** call. ▪ **[0]** Disable ▪ **[1]** Enable (default)
Periodic Inform Interval **[management/tr069/inform/interval]**	The duration (in seconds) of the interval for which the device must attempt to connect with the ACS and call the **Inform method** if TR-069 is enabled (**management/tr069/inform/enabled**). The valid range is 0 to 86400. The default is 3600.

Part II

Automatic Provisioning

Reader's Notes

6   Introduction

By default, the IP phone is ready for out-of-the-box deployment using its automatic provisioning capabilities.

The IP phone offers a built-in mechanism for automatically upgrading its software image and updating its configuration. This method is used to upgrade the phone firmware and update its configuration, by remotely downloading an updated software image and configuration file.

The automatic update mechanism helps you keep your software image and configuration up-to-date, by performing routine checks for newer software versions and configuration files, as well as allowing you to perform manual checks.

The automatic update mechanism is as follows:

■   Before connecting the phone, verify that the provisioning server is running and that the firmware and configuration files are located in the correct location.

■   Connect your phone to the IP network, and then connect the phone to the power outlet.

■   During DHCP negotiation, the phone requests for DHCP options 66/67/160 to receive provisioning information. The DHCP server should respond with Option 160 providing the provisioning URL or Options 66 and 67 providing the TFTP IP address and firmware file name respectively.

■   The phone then checks whether new firmware is available by checking the firmware file header. If the version is different from the one currently running on the phone, the phone downloads the complete image and burns it to its flash memory.

■   If a new firmware is unavailable, the phone then checks whether a new configuration is available. If a configuration file is available on the server, the phone downloads it and updates the phone's configuration after verifying that the configuration file is related to the phone model. When a configuration update is needed, the phone might reboot.

> **Notes:**
>
> - In the DHCP Discover message, the phone publishes its model name in Option fields 60 and 77 (e.g. 320HD). If the administrator wants to provide different provisioning information to different phone models, the administrator can set up a policy in the DHCP server according to the phone model name.
>
> - If the phone for some reason is powered off during the firmware upgrade process, the phone is unusable and the recovery process must be performed (see Section 40 on page 255).
>
> - You can only use firmware files with an *.img* extension and configuration files with a *.cfg* extension.
>
> - To "force" the firmware or configuration file to be retrieved immediately regardless of the "Check Period" value, click the **Check Now** button on the relevant page on the Web interface.
>
> - An additional auto-provisioning mechanism is supported if the provisioning environment does not provide all the required information (e.g. DHCP options).

Reader's Notes

7   Updating (Manually) Configuration File

The phone enables you to view, save, and load its configuration file to backup and restore the current configuration.

➢ **To manually update the configuration file:**

1. Access the 'Configuration File' page (**Management** tab > **Manual Update** menu > **Configuration File**). The current configuration file settings are displayed in the text pane.

Figure 7-1: Configuration File Web Fields

2. Click the **Loading new Configuration File** button; the following page appears:

Figure 7-2: Load New Configuration File Web Field

3. Click the **Browse** button and then select the required configuration file located on your local PC; the phone verifies that the configuration file is related to the phone model. The configuration file is then loaded to the phone. Once loaded, the phone reboots (indicated by a message displayed on the phone's screen). The phone is now updated with the new configuration.

> **Note:** The configuration file name must have the extension *.cfg.*

➢ **To save the configuration file:**

■ In the 'Configuration File' page, click the **Saving Current Configuration File** button, and then save the current phone configuration file to a folder on your local PC.

> **Note:** When creating a new configuration file, ensure that the *system/type* parameter in the configuration file is set to the proper phone model (e.g.,320HD).

Reader's Notes

8   Setting up Network for Auto Provisioning

The IP Phone supports dynamic VLAN discovery, Dynamic IP addressing (DHCP), and NTP (as client).

⚠️	**Note:** For manual configuration of Network Settings, see Section 13 on page

Reader's Notes

9   Obtaining Firmware and Configuration

The Web interface allows you to perform the following:

- Automatic update of firmware and configuration files
- Manual update of firmware and configuration files

9.1   Methods

There are three different ways of configuring automatic provisioning:

- DHCP
- Static DNS Record
- Using SIP SUBSCRIBE and NOTIFY Messages

9.1.1   DHCP

Dynamic Host Configuration Protocol (DHCP) can be used to configure automatic provisioning. The DHCP feature can be configured using the Web or Configuration File, as described below

➢ **To configure with DHCP:**

- **Using the Web:**
    1. Access the 'Automatic Update page (**Management** tab > **Automatic Update** menu > **Automatic Provisioning**).

Figure 9-1: Automatic Provisioning Web Fields

Firmware Version :	1.4.1_build_32
Provisioning Method :	DHCP Options (Dynamic URL)
Dynamic Firmware URL :	tftp://ProvisioningServer/320HD/320HD.img [Check Now]
Dynamic Configuration URL :	tftp://ProvisioningServer/320HD/00908f1ed2f0.cfg [Check Now]
DHCP Option Value :	160
Check Period :	Daily
Every day at :	00:00
Random Provisioning Time :	120 minutes

    2. Configure automatic update of firmware and configuration files according to the parameters in the table below, and then click **Submit**.

■ **Using the Configuration File:**

Table 9-1: Automatic Update Methods Parameters

Parameter	Description
Note: To add a value to these parameters, enter `provisioning/` followed by the parameter name equals the value (e.g. `provisioning/method=dynamic`).	
Provisioning Method **[provisioning/method]**	Defines the provisioning method: ▪ **[Disable]** Disable - Automatic update is disabled. The phone attempts to upgrade its firmware and configuration ▪ **[Dynamic]** DHCP Options (Dynamic URL) (default) - Using DHCP options 160 or 66/67 for provisioning ▪ **[Static]** Static URL - Using Static URL for provisioning
DHCP Option Value **[provisioning/url_option_value]**	Determines the DHCP option number to be used for receiving the URL for provisioning. The default value is 160. The phone supports DHCP Option 160 for complete URL and Options 66/67 for TFTP usage. Option 160 has the highest priority and if absent, Options 66/67 are used. The following syntax is available for DHCP option 160: ▪ <protocol>://<server IP address or host name> ▪ <protocol>://<server IP address or host name>/<firmware file name> ▪ <protocol>://<server IP address or host name>/<firmware file name>;<configuration file name> ▪ <protocol>://<server IP address or host name>/;<configuration file name> Where <protocol> can be one of the following: "ftp", "tftp", "http" or "https". For example: ▪ **ftp://192.168.2.1** – retrieved firmware file is *310HD.img* and the configuration file name is <MAC address>.cfg. For example, 001122334455.cfg ▪ **tftp://192.168.2.1/different_firmware_name.img** - retrieved firmware file is Different_Firmware_Name.img and the configuration file name is <MAC address>.cfg. For example, 001122334455.cfg ▪ **http://192.168.2.1/different_firmware_name.img ; 310HD_<MAC>_conf.cfg** - retrieved firmware file is different_firmware_name.img and the configuration file name is 310HD_<MAC address>_conf.cfg. For example, **310HD_001122334455_conf.cfg** • **https://192.168.2.1/310HD_<MAC>_conf.cfg** - In this case the retrieved firmware file is 310HD.img and the configuration file name is 310HD_<MAC

Parameter	Description
	Address>_conf.cfg. For example, 310HD_001122334455_conf.cfg The following syntax is available for DHCP Options 66/67: ▪ Option 66 must be a valid IP address or host name of a TFTP server only. ▪ Option 67 must be the firmware name. If Option 67 is absent, the phone requests for the 310HD.img image file. For example: ▪ **Option 66:** 192.168.2.1 or myTFTPServer ▪ **Option 67:** 310HD_1.2.2_build_5.img **Notes:** ▪ This parameter is applicable only when **method** is configured to "Dynamic". It is recommended to leave the parameter at its default value to avoid conflict with other DHCP options settings.
Random Provisioning Time **[provisioning/random_provisioning_time]**	Defines the maximum random number to start the provisioning process. This is used for periodic checking of firmware and configuration files to avoid multiple devices from starting the upgrade process at the same time. When the device is meant to start the upgrade, the device randomly selects a number between 1 and the value set for **random_provisioning_time** and performs the check only after the random time. The valid range is 0-65535. The default value is 120.
Check Period **[provisioning/period/type]**	Defines the period type for automatic provisioning: ▪ **[hourly]** Hourly **-** Sets an interval in hours. ▪ **[daily]** Daily (default) - Sets an hour in the day. ▪ **[weekly]** Weekly - Sets a day in the week and an hour in the day. ▪ **[powerup]** On Power-up Only - The phone tries to upgrade only after power-up.
Every (Check Period = Hourly) **[provisioning/period/hourly/hours_interval]**	The interval in hours for automatically checking for new firmware and configuration files. The valid range is 1 to 168. The default is 24. **Note:** This parameter is applicable only when `type` is configured to "hourly".
Every day at **[provisioning/period/daily/time]**	The hour in the day for automatically checking for new firmware and configuration files. The format of this value is **hh:mm**, where **hh** is hour and **mm** is minutes. For example, `00:30`**.** The default time is **00:00**. **Note:** This parameter is applicable only when **type** is configured to "daily".
Every (Check Period = Day) **[provisioning/period/weekly/day]**	The day in the week for automatically checking for new firmware and configuration files.

Parameter	Description
	▪ **[Sunday]** Sunday (default) ▪ **[Monday]** Monday ▪ **[Tuesday]** Tuesday ▪ **[Wednesday]** Wednesday ▪ **[Thursday]** Thursday ▪ **[Friday]** Friday ▪ **[Saturday]** Saturday **Note:** This parameter is applicable only when **type** is configured to "weekly".
Every (Check Period = Weekly) **[provisioning/period/weekly/time]**	The hour in the day for automatically checking for new firmware and configuration files. The format of this value is: **hh:mm**, where **hh** is hour and **mm** is minutes. For example: **00:30** The default time is **00:00**. **Note:** This parameter is applicable only when **type** is configured to "weekly".
provisioning/XXX_uri	The URI that allows the administrator to retrieve relevant information from separate files. The URI's can include specific protocol and path of the provisioning server or alternatively, the files can be retrieved from the server whose information was provided during provisioning (e.g. DHCP options 66/67 or 160). For example, in the below setting, *YYY.ext* is retrieved from the server whose information was provided during provisioning (e.g. DHCP options 66/67 or 160: **provisioning/XXX_uri=YYY.ext** Alternatively, the full URL and protocol can be set as follows: **provisioning/XXX_uri=<protocol>://<full path>/YYY.ext** For example: ▪ provisioning/XXX_uri=tftp://10.10.10.10/YYY.ext ▪ provisioning/XXX_uri=ftp:// 10.10.10.10/YYY.ext ▪ provisioning/XXX_uri=http:// 10.10.10.10/YYY.ext ▪ provisioning/XXX_uri=https:// 10.10.10.10/YYY.ext

9.1.1.1   Configuring DHCP Option 160

DHCP Option Value 160 can be configured using the Web as shown below.

➢ **To configure DHCP Option 160:**

■ **Using the Web:**

    1. Access the 'Automatic Update page (**Management** tab > **Automatic Update** menu > **Automatic Provisioning**).

Figure 9-2: Automatic Provisioning - DHCP Option 160 Web Fields

    2. From the 'Provisioning Method' drop-down list, select **DHCP Option (Dynamic URL)**.

    3. In the 'DHCP Option Value' field, enter "160".

    4. Configure the remaining parameters, and then click **Submit**.

    5. After reboot, confirm that the firmware and configuration files have been updated.

9.1.1.2   Configuring DHCP Options 66 and 67

DHCP Options 66 and 67 can be configured using the Web as shown below.

➢ **To configure DHCP Options 66 and 67:**

■ **Using the Web:**

    1. Access the 'Automatic Update page (**Management** tab > **Automatic Update** menu > **Automatic Update**).

Figure 9-3: Automatic Provisioning - DHCP Options 66/67 Web Fields

    2. From the 'Provisioning Method' drop-down list, select **DHCP Option (Dynamic URL)**.

    3. In the 'DHCP Option Value' field, enter "0".

    4. Configure the remaining parameters, and then click **Submit**.

    5. After reboot, confirm that the firmware and configuration files have been updated.

9.1.2   Static DNS Record (Generic Domain Name)

This method is used for automatic provisioning when you are unable to manage your DHCP server. If the provisioning server does not support using SIP SUBSCRIBE and NOTIFY messages mechanism as described above and no response for the SIP SUBSCRIBE message has been received, the phone tries to retrieve firmware and configuration files using the following URL: **tftp://ProvisioningServer/<Phone Model Name>/**

For example:

■   The phone tries to obtain the following firmware file:
      tftp://ProvisioningServer/310HD/310HD.img

■   The phone tries to obtain the following configuration file:
      tftp://ProvisioningServer/310HD/<MAC address>.cfg

      (e.g. tftp://ProvisioningServer/310HD/001122334455.cfg)

It is the Administrator's responsibility to configure a DNS entry called **ProvisioningServer** on the DNS server and set it to the TFTP server IP address.

> **Note:** If Generic Domain Name is used, the automatic provisioning mechanism periodically tries to retrieve new firmware/configuration from Provisioning Server domain name.

➢   **To configure Static DNS Record:**

■   **Using the Web:**

    1.   Access the 'Automatic Update page (**Management** tab > **Automatic Update** menu > **Automatic Provisioning**).

Figure 9-4: Static DNS Record Web Fields

Firmware Version :	1.6.0_build_37_4	
Provisioning Method :	Static URL	
Firmware URL :	ftp://10.16.2.40/pilot_310.img	Check Now
Configuration URL :		Check Now
Check Period :	Daily	
Every day at :	00:00	
Random Provisioning Time :	120 minutes	

    2.   Configure Static DNS Record according to the parameters in the table below, and then click **Submit**.

■   **Using the Configuration file:**

Table 9-2: Static DNS Record Parameters

Parameter	Description
Firmware URL **[provisioning/firmware/url]**	The static URL for checking the firmware file. The URL must be entered using one of the following syntax options: ▪ <protocol>://<server IP address or host name> ▪ <protocol>://<server IP address or host name>/<firmware file name> Where <protocol> can be one of the following protocols: "ftp", "tftp", "http" or "https". For example: ▪ tftp://192.168.2.1 – retrieved firmware file is 310HD.img ▪ ftp://192.168.2.1/Different_Firmware_Name.img - retrieved firmware file is Different_Firmware_Name.img **Note:** This parameter is applicable only when **method** is configured to "Static".
Configuration URL **[provisioning/configuration/url]**	The static URL for checking the configuration file. The URL must be entered using one of the following syntax options: ▪ <protocol>://<server IP address or host name> ▪ <protocol>://<server IP address or host name>/<configuration file name> Where <protocol> can be one of the following protocols: "ftp", "tftp", "http" or "https". For example: ▪ http://192.168.2.1 - configuration file name is <MAC Address>.cfg, for example, 001122334455.cfg ▪ https://192.168.2.1/310HD_<MAC>_conf.cfg - retrieved configuration file name is 310HD_<MAC Address>_conf.cfg, for example, 310HD_001122334455_conf.cfg **Note:** This parameter is applicable only when **method** is configured to "Static".

9.1.3   SIP SUBSCRIBE and NOTIFY Messages

If the provisioning information (e.g. Option fields 66/67/160) is not provided by the DHCP server, the phone sends a SIP SUBSCRIBE message to the multicast address **224.0.1.75:5060** as shown below.

> ⚠️ **Note:** If the provisioning server supports using SIP SUBSCRIBE and NOTIFY messages and the device receives the provisioning URL in the NOTIFY message, the automatic provisioning mechanism then periodically tries to retrieve a new firmware/configuration according to the information provided.

```
SUBSCRIBE sip:224.0.1.75:5060 SIP/2.0
From: <sip:00000001@10.13.2.37:5060>;tag=87a5a8-25020d0a-13c4-
50029-386d4398-66dc40c-386d4398
To: <sip:224.0.1.75:5060>
Call-ID: 8884c8-25020d0a-13c4-50029-386d4398-3e2bcb8e-386d4398
CSeq: 1 SUBSCRIBE
Via: SIP/2.0/UDP 10.13.2.37:5060;rport;branch=z9hG4bK-386d4398-
6ad00ca2-7ca3606e
Expires: 0
Event: ua-profile;profile-
type="application";model="310HD";version="1.2.1_build_6"
Max-Forwards: 70
Supported: replaces,100rel
Accept:  application/url
Contact: <sip:00000001@10.13.2.37:5060>
User-Agent: AUDC-IPPhone/1.2.1_build_6
Content-Length: 0
```

The provisioning server or any other entity replies with a 200 OK message to the SUBSCRIBE message (see below) and sends a NOTIFY SIP message with the provisioning URL in the message body as shown below. (The provisioning URL can be in any format as described in the Administrator's Manual).

If no response is received by the provisioning server, the phone resends SUBSCRIBE messages for five seconds.

With the above method, the phone uses its built-in auto-provisioning mechanism while the provisioning information is retrieved through the NOTIFY message.

The following code describes **SIP 200 OK Response on the SUBSCRIBE Message**:

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.13.2.37:5060;rport;branch=z9hG4bK-386d4398-
6ad00ca2-7ca3606e
Contact: <sip:10.13.2.37:5060>
To: <sip:224.0.1.75:5060>
From: <sip:00000001@10.13.2.37:5060>;tag=87a5a8-25020d0a-13c4-
50029-386d4398-66dc40c-386d4398
Call-ID: 8884c8-25020d0a-13c4-50029-386d4398-3e2bcb8e-386d4398
CSeq: 1 SUBSCRIBE
Expires: 0
Content-Length: 0
```

The following code describes **SIP NOTIFY Message with Provisioning Information**.

```
NOTIFY sip:10.13.2.37:5060 SIP/2.0
```

```
Via: SIP/2.0/UDP 10.13.2.37:5060;rport;branch=z9hG4bK-386d4398-
6ad00ca2-7ca3606e
Max-Forwards: 20
Contact: <sip:10.13.4.121:5060>
To: <sip:224.0.1.75:5060>
From: <sip:00000001@10.13.2.37:5060>;tag=87a5a8-25020d0a-13c4-
50029-386d4398-66dc40c-386d4398
Call-ID: 8884c8-25020d0a-13c4-50029-386d4398-3e2bcb8e-386d4398
CSeq: 1 NOTIFY
Content-Type: application/url
Subscription-State: terminated;reason=timeout
Event: ua-profile;profile-
type="application";model="310HD";version="1.2.0"
Content-Length: 18
tftp://10.13.4.121
```

The following code describes **SIP SUBSCRIBE Message to Obtain Provisioning Information.**

```
SUBSCRIBE sip:224.0.1.75:5060 SIP/2.0
From: <sip:00000001@10.13.2.37:5060>;tag=87a5a8-25020d0a-13c4-
50029-386d4398-66dc40c-386d4398
To: <sip:224.0.1.75:5060>
Call-ID: 8884c8-25020d0a-13c4-50029-386d4398-3e2bcb8e-386d4398
CSeq: 1 SUBSCRIBE
Via: SIP/2.0/UDP 10.13.2.37:5060;rport;branch=z9hG4bK-386d4398-
6ad00ca2-7ca3606e
Expires: 0
Event: ua-profile;profile-
type="application";model="310HD";version="1.2.1_build_6"
Max-Forwards: 70
Supported: replaces,100rel
Accept:  application/url
Contact: <sip:00000001@10.13.2.37:5060>
User-Agent: AUDC-IPPhone/1.2.1_build_6
Content-Length: 0
```

The provisioning server or any other entity replies with a 200 OK message to the SUBSCRIBE message (see below) and sends a NOTIFY SIP message with the provisioning URL in the message body as shown below. (The provisioning URL can be in any format as described in the Administrator's Manual).

If no response is received by the provisioning server, the phone resends SUBSCRIBE messages for 5 seconds.

With the above method, the phone uses its built-in auto-provisioning mechanism while the provisioning information is retrieved through the NOTIFY message.

The following code describes **SIP 200 OK Response on the SUBSCRIBE Message.**

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.13.2.37:5060;rport;branch=z9hG4bK-386d4398-
6ad00ca2-7ca3606e
Contact: <sip:10.13.2.37:5060>
To: <sip:224.0.1.75:5060>
From: <sip:00000001@10.13.2.37:5060>;tag=87a5a8-25020d0a-13c4-
50029-386d4398-66dc40c-386d4398
Call-ID: 8884c8-25020d0a-13c4-50029-386d4398-3e2bcb8e-386d4398
CSeq: 1 SUBSCRIBE
Expires: 0
Content-Length: 0
```

The following code describes **SIP NOTIFY Message with Provisioning Information.**

```
NOTIFY sip:10.13.2.37:5060 SIP/2.0
Via: SIP/2.0/UDP 10.13.2.37:5060;rport;branch=z9hG4bK-386d4398-
6ad00ca2-7ca3606e
Max-Forwards: 20
Contact: <sip:10.13.4.121:5060>
To: <sip:224.0.1.75:5060>
From: <sip:00000001@10.13.2.37:5060>;tag=87a5a8-25020d0a-13c4-
50029-386d4398-66dc40c-386d4398
Call-ID: 8884c8-25020d0a-13c4-50029-386d4398-3e2bcb8e-386d4398
CSeq: 1 NOTIFY
Content-Type: application/url
Subscription-State: terminated;reason=timeout
Event: ua-profile;profile-
type="application";model="310HD";version="1.2.0"
Content-Length: 18
tftp://10.13.4.121
```

9.2   Protocols for Acquiring Files

You can load various files to the IP phone such as CFG files, Certification Files, Speed Dial files, and Tones files using the following protocols:

- HTTP/S
- TFTP
- FTP

Reader's Notes

Part III

Quick Setup

Reader's Notes

10   Quick Setup

The Web interface provides you with a Quick Setup page that allows you to configure basic features to quickly set up your IP Phone to operational level.

> **Note:**   For descriptions of these quick setup parameters, see Part IV (Networking) and Part V (VoIP Features).

➢ **To quickly setup your phone:**

1.   Access the 'Quick Setup' page (**Configuration** tab > **Quick Setup** menu > **Quick Setup**).

Figure 10-1: Quick Setup Web Fields

LAN Setup	
IP Type:	○ Static IP ⦿ Automatic IP (DHCP)
IP Address:	10.13.10.10
Subnet Mask:	255.255.0.0
Default Gateway Address:	10.13.0.1
Primary DNS:	0.0.0.0
Secondary DNS:	0.0.0.0

SIP Proxy and Registrar	
Use SIP Proxy:	Enable
Proxy IP Address or Host Name:	10.16.2.56
Proxy Port:	5060
Use SIP Proxy IP and Port for Registration:	Enable
Use SIP Registrar:	Disable

Line Settings	
Line Number:	1
Line 1 Activate:	Enable
Line 1 Display Name:	310HD
Line 1 User ID:	201
Line 1 Authentication User Name:	201
Line 1 Authentication Password:	•••

2.   For a description of the parameters on this page, refer to the following:

- Parameters under the **LAN Setup** group, see Section 13.1.2 on page 78.
- Parameters under the **SIP Proxy and Registrar** group see Section 17.2 on page 93.
- Parameters under the **Line Settings** group, see Section 21.2 on page 132.

Reader's Notes

Part IV

Networking

Reader's Notes

11   Introduction

This part describes manual network settings, if required.

	Note: By default the network settings are set for automatic provisioning. However, if you need to change them, you can do it manually as is described in this part.

Reader's Notes

12   Configuring Date and Time

Generally, a phone retrieves the date and time from a Network Time Protocol (NTP) server when it connects to the Internet. Alternatively, the date and time can be configured manually. NTP is a protocol for distributing the Coordinated Universal Time (UTC) by means of synchronizing the clocks of computer systems over packet-switched, variable-latency data networks.

> **Note:** By default, the network settings are configured for automatic provisioning. However, if you need to change them, you can do it manually as is described in this part.

12.1   Configuring Date and Time

The date and time can be configured using the Web or Configuration File, as described below.

➢   **To configure the date and time:**

■   **Using the Web:**

1.   Access the 'Date and Time' page (**Configuration** tab > **Advanced Applications** menu > **Date and Time**).

Figure 12-1: Date and Time Web Fields

2.   Configure the date and time according to the parameters in the table below, and then click **Submit**.

■ **Using the Configuration File:**

Table 12-1: Daylight Saving Time Parameters

Parameter	Description
Active **[system/daylight_saving/activate]**	Determines whether the phone automatically detects the Daylight Saving setting for selected time zones. ▪ **[Disable]** Disable (default) ▪ **[Enable]** Enable
Start Time **[system/daylight_saving/start_date]**	This sub-section defines the starting day for the daylight saving offset. ▪ **[month]** - defines the specific month in a year ▪ **[day]** - defines the specific day in a month ▪ **[hour]** - defines the specific hour in a day ▪ **[minute]** - defines the specific minute in an hour For example: To configure the phone to start daylight savings with a specific offset on February 22nd at 14:30, set the following: **system/daylight_saving/start_date/month=2** **system/daylight_saving/start_date/day=22** **system/daylight_saving/start_date/hour=14** **system/daylight_saving/start_date/minute=30**
Start Time **[system/daylight_saving/start_date/month]**	The month in a year. The valid range is 1 to 12.
Start Time **[system/daylight_saving/start_date/day]**	The day in a month. The valid range is 1 to 31.
Start Time **[system/daylight_saving/start_date/hour]**	The hour in the day. The valid range is 0 to 23.
Start Time **[system/daylight_saving/start_date/minute]**	The minute in an hour. The valid range is 0 to 59.

Parameter	Description
End Time **[system/daylight_saving/end_date]**	This sub-section defines the ending day for the daylight saving offset. ▪ **[month]** - defines the specific month in a year ▪ **[day]** - defines the specific day in a month ▪ **[hour]** - defines the specific hour in a day ▪ **[minute]** - defines the specific minute in an hour For example: To configure the phone to end the daylight savings on July 16th at 22:15, set the following: **system/ntp/daylight_saving/end_date/month =7** **system/ntp/daylight_saving/end_date/day=16** **system/ntp/daylight_saving/end_date/hour=2 2** **system/ntp/daylight_saving/end_date/minute =15**
End Time **[system/daylight_saving/end_date/month]**	The month in a year. The valid range is 1 to 12.
End Time **[system/daylight_saving/end_date/day]**	The day in a month. The valid range is 1 to 31.
End Time **[system/daylight_saving/end_date/hour]**	The hour in the day The valid range is 0 to 23.
End Time **[system/daylight_saving/end_date/minute]**	The minute in an hour. The valid range is 0 to 59.
Offset **[system/daylight_saving/offset]**	The offset value for the daylight saving. The valid range is 0 to 180. The default offset is 60.
/system/daylight_saving/mode	Configures the daylight saving mode. Valid values are **[Fixed]=** Date is specified as: Month, Day of month. **[DayOfWeek]=** Date is specified as: Month, Week of month, Day of week.
/system/daylight_saving/start_date/week	Relevant to "Day of week" mode: The week of month (values 1-5) for start of daylight saving time.

Parameter	Description
/system/daylight_saving/start_date/day_of_week	Relevant to "Day of week" mode: The day of week for daylight saving time start Valid values : **[SUNDAY]** **[MONDAY]** **[TUESDAY]** **[WEDNESDAY]** **[THURSDAY]** **[FRIDAY]** **[SATURDAY]**
/system/daylight_saving/end_date/week	Relevant to "Day of week" mode: The week of month (values 1-5) for end of daylight saving time.
/system/daylight_saving/end_date/day_of_week	Relevant to "Day of week" mode: The day of week for daylight saving time start Valid values : **[SUNDAY]** **[MONDAY]** **[TUESDAY]** **[WEDNESDAY]** **[THURSDAY]** **[FRIDAY]** **[SATURDAY]**

12.2   Configuring Network Time Protocol Server

The Network Time Protocol (NTP) server can be configured using the Web or Configuration File, as described below.

➢ **To configure the Network Time Protocol Server:**

■ **Using the Web:**

1. Access the 'Date and Time' page (**Configuration** tab > **Advanced Applications** menu > **Date and Time**).

2. Configure the Network Time Protocol Server according to the parameters in the table below, and then click **Submit**.

Figure 12-2: NTP and Time Settings Web Fields

■ **Using the Configuration File:**

Table 12-2: NTP Server Parameters

Parameter	Description
Active **[system/ntp/enabled]**	Enables the NTP server from which the phone retrieves the date and time. ▪ **[0]** Disable (default) ▪ **[1]** Enable – obtains the time information from a configured NTP server
Primary Server **[system/ntp/primary_server_address]**	Defines the address of the main NTP server (this can be a domain name, for example, tick.nap.com.ar).
Secondary Server **[system/ntp/secondary_server_address]**	Defines the address of the secondary NTP server.
Update Interval **[system/ntp/sync_time]**	This sub-section defines how often the phone must perform an update with the NTP server. ▪ **[days]** - defines the number of days ▪ **[hours]** - defines the number of hours For example: To configure the phone to perform an update with an NTP server every 1 day and 6 hours, set the following: **system/ntp/sync_time/days=1** **system/ntp/sync_time/hours=6**
Update Interval **[system/ntp/sync_time/days]**	The number of days. The valid range is 0 to 7. The default of days is 0.

Parameter	Description
Update Interval **[system/ntp/sync_time/hours]**	The number of hours. The valid range is 0 to 24. The default is 12.
Time Display Format **[system/ntp/time_display_format]**	The format of the time displayed on the LCD screen. ▪ **[24Hour]** (default) ▪ **[12Hour]**

12.3   Configuring Network Time Protocol Server via DHCP

If the IP Phone is set to obtain GMT offsets and NTP servers via DHCP (default), it receives the following fields in the DHCP options:

■   Primary Server and Secondary Server – (Option 4 or 42).

> **Note:**   If both options (4 and 42) are received, the higher priority is given to Option 42.

■   Time Zone – (Option 2)

The IP Phone sends an NTP request to the Primary NTP server. If there is no response, the NTP request is sent to the Secondary NTP server.

After obtaining the time from the server it adds the GMT offset in Option 2 and this is the updated system time.

➢   **To manually configure the NTP Server and GMT offset via DHCP:**

■   **Using the Web:**

1.   Access the 'Date and Time' page (**Configuration** tab > **Advanced Applications** menu > **Date and Time**).
2.   From the "Obtain Time Zone From DHCP" drop-down list, select **Disable**.
3.   Configure the NTP and Time Settings according to the parameters in the table below, and then click **Submit**.

> **Note:**   These values will have no affect if the timezone is set to be obtained from DHCP. If the Time Zone and NTP servers are manually set, the IP Phone acts the same as described above, but the values are obtained from configuration file and not from DHCP.

Figure 12-3: NTP and Time Settings Web Fields

Table 12-3: NTP Server and GMT Parameters

Parameter	Description
[network/lan/dhcp/ntp/gmt_offset]	Enables the NTP server from which the phone retrieves the date and time. ▪ **[0]** Disable (default) ▪ **[1]** Enable – obtains the time information from a configured NTP server

Reader's Notes

13   IP Network Settings

The following section describes how to configure IP Network Settings including:

- Static IP Address
- Partial DHCP

13.1   Configuring Static IP Address

The static IP address can be configured using the following:

- Phone User Interface
- Web and Configuration File

13.1.1   Configuring the Static IP Address using Phone User Interface

The procedures for configuring the Static IP Address on the 310HD IP Phone, 320HD IP Phone and 420HD IP Phone using the Phone User Interface, are described below.

13.1.1.1 310HD IP Phone

The phone's LAN connection interface can be manually defined (static IP address) or automatically configured using a DHCP server from where the LAN IP address is obtained.

➢ **To configure the phone's LAN connection type:**

1. Access the Network Settings screen (**MENU** key > **Administration** menu > **Network Settings** > **LAN Conn. Type**).
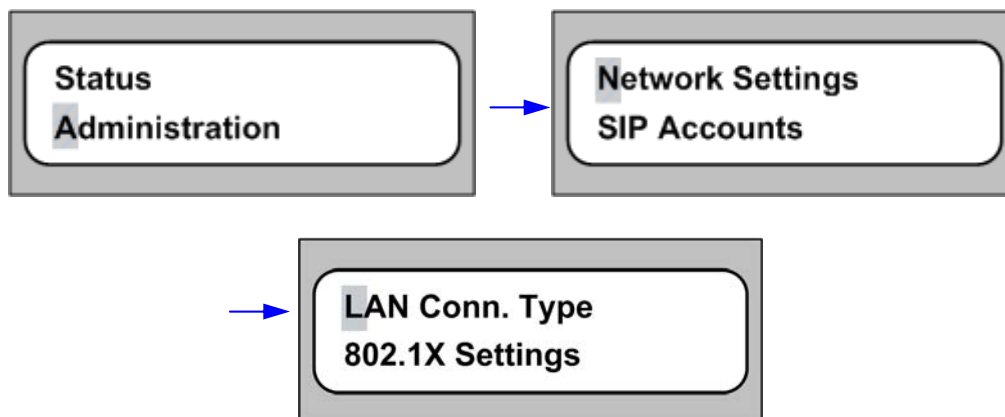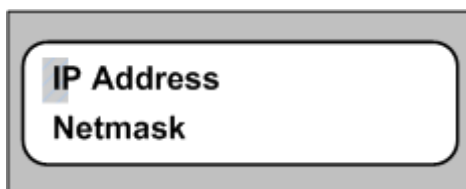
The following screen appears:
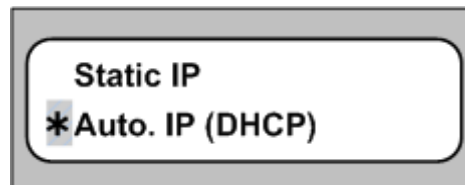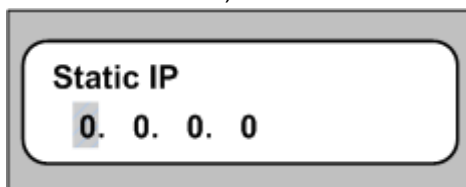
2. Choose one of the following IP addressing schemes (using the ▲ and ▼ Navigation keys), and then press the ENTER key (the asterisk appears alongside your selection):

    - Static IP
    - Auto. IP (DHCP)

3. Press the ENTER key again. If you selected **Static IP**, then continue with Step 4; otherwise, skip to Step 5.

4. If you selected the **Static IP** option, the following screen appears:
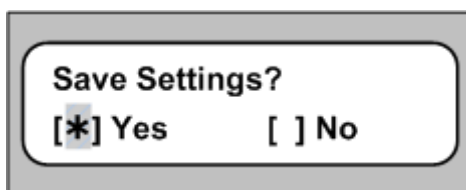
```
IP Address
Netmask
```

a. Select the required network parameter (**IP Address**, **Netmask**, **Gateway**, **Primary DNS**, and/or **Secondary DNS**), and then press the ENTER key; the screen prompts you to enter the IP address of the selected network parameter (e.g., static IP address below):

```
Static IP
  0.  0.  0.  0
```

b. Enter the required value, and then press the ENTER key; the setting is applied.

c. Repeat steps 4.a through 4.c for each required network parameter.

5. Press the left ◄ Navigation key until you are prompted to save settings, as shown below:

```
Save Settings?
[*] Yes        [ ] No
```
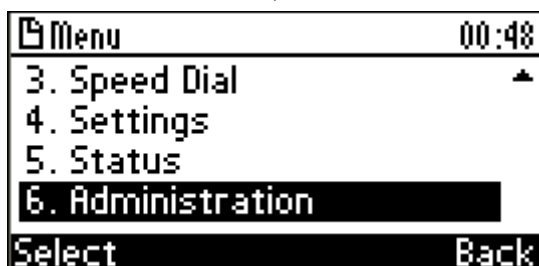
6. Select the **Yes** option (using the ◄ and ► Navigation keys), and then press the ENTER key; the network settings are saved.

13.1.1.2 320HD IP Phone

The phone's LAN connection interface can be manually defined (static IP address) or automatically provisioned using a DHCP server from where the LAN IP address is obtained.

➢ **To configure the phone's LAN connection type:**
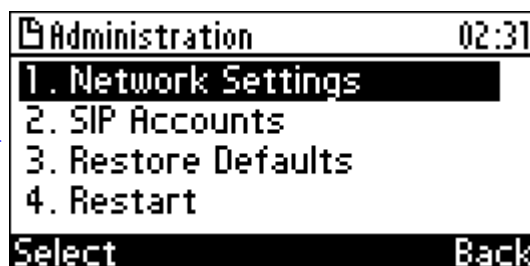
1. Access the Settings screen (MENU key > **Administration** menu > **Network Settings** submenu).

```
📄Menu                00:48
 3. Speed Dial          ▲
 4. Settings
 5. Status
 6. Administration
Select              Back
```
→
```
📄Administration      02:31
 1. Network Settings
 2. SIP Accounts
 3. Restore Defaults
 4. Restart
Select              Back
```

The following screen appears:

```
┌──────────────────────────────┐
│ ▯Settings              21:07 │
│ ████████████████████████████ │
│ 1.LAN Connection Type        │
│ 2.802.1X Settings            │
│                              │
│                              │
│                              │
│ Select                  Back │
└──────────────────────────────┘
```

2. Using the ▲ and ▼ Navigation keys, choose **LAN Connection Type**, and then press the **Select** softkey; the following screen appears:

```
┌──────────────────────────────┐
│ ▯Settings            01:54AM │
│ ○Static IP                   │
│ ⦿Automatic IP (DHCP)         │
│                              │
│                              │
│                              │
│ Select          Save    Back │
└──────────────────────────────┘
```
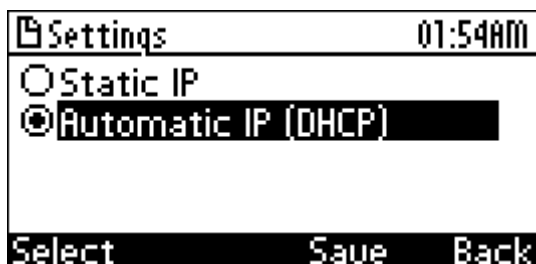
3. Using the ▲ and ▼ Navigation keys, choose one of the following IP addressing schemes:

- **Static IP**
- **Automatic IP (DHCP)**

4. Press the **Select** softkey. If you selected "Static IP" in Step 3, continue with Step 5; otherwise, skip to Step 6.

5. Define a static IP addressing scheme:

   a. Press the **Edit** softkey; the Static IP screen appears:

```
┌──────────────────────────────┐
│ ▯Static IP           02:06AM │
│ ████████████████████████████ │
│ Static IP                    │
│    0.0.0.0                   │
│ Netmask                      │
│    0.0.0.0                  ▼│
│          Edit   Apply   Back │
└──────────────────────────────┘
```
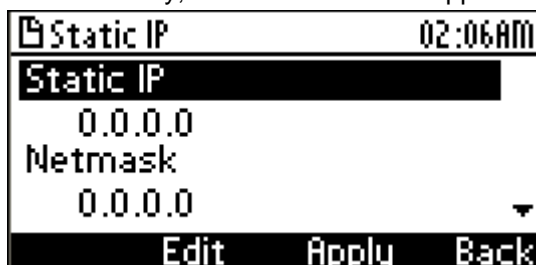
   b. To configure each required network parameter (i.e., "IP Address", "Netmask", "Gateway", "Primary DNS", and "Secondary DNS"), choose the parameter using the ▲ and ▼ Navigation keys, and then press the **Edit** softkey. Enter the new address in dotted-decimal notation, using the following keys:

   ♦ **Navigation keys:** moves the cursor left or right in the IP address
   ♦ **Clear softkey:** deletes the digit to the left of the cursor.

   c. Press the **Save** and then **Apply** softkey.

6. Press the **Save** softkey.

13.1.1.3 420HD IP Phone

The procedure for configuring Static IP Address on the 420HD IP Phone using the Phone User Interface is identical to that for the 320HD IP Phone. The phone's LAN connection interface can be manually defined (static IP address) or automatically provisioned using a DHCP server from where the LAN IP address is obtained.

➢ **To configure the phone's LAN connection type:**

1. Access the Settings screen (**MENU** key > **Administration** > **Network Settings**).

```
Menu                          Administration
 5. Status                     1. Network Settings
 6. Administration             2. SIP Accounts
Select              Back      Select              Back
```

```
Settings
 1. LAN Connection Type
 2. 802.1X Settings
Select              Back
```
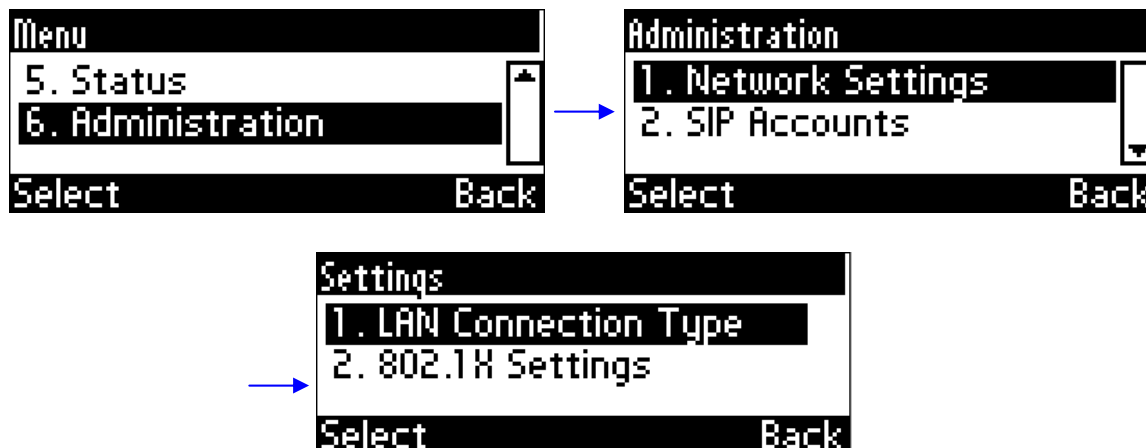
2. Press the **Select** softkey to select **LAN Connection Type**; the Settings prompt is displayed:

```
Settings                      Settings
 ⊙ Static IP                   ○ Static IP
 ○ Automatic IP (DHCP)         ⊙ Automatic IP (DHCP)
Select  Edit  Save  Back      Select      Save  Back
```

3. Press the navigation control's lower rim to navigate to **Static IP** or **Automatic IP (DHCP)** IP addressing scheme.

4. Press the **Select** softkey. If you selected **Static IP** in Step 3, continue with Step 5; else skip to Step 6.

5. Define a static IP addressing scheme:

   a. Press the **Edit** softkey; the Static IP screen appears:

```
Static IP
 IP Address
     0.0.0.0
        Edit   Apply   Back
```

   b. To configure each required network parameter, i.e., **IP Address**, **Netmask**, **Gateway**, **Primary DNS** and **Secondary DNS**, choose the parameter using the navigation control's lower or upper rim to navigate to it, and then press the **Edit** softkey, for example, navigate to **IP Address** and press the **Edit** softkey:

```
Static IP
  Static IP
  0.0.0.0|
            Clear    Saue    Back
```
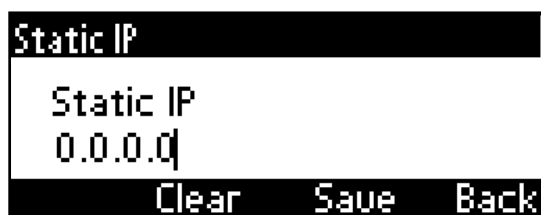
       c.   Enter the new address in dotted-decimal notation, using the following keys:

           ♦   **Navigation control:** moves the cursor left or right in the IP address

           ♦   **Clear** softkey**:** deletes the digit to the left of the cursor.

       d.   Press the **Save** and then **Apply** softkey.

    6.   Press the **Save** softkey.

13.1.2 Configuring IP Network Settings using Web and Configuration File

This section describes how to configure IP Network settings using the Web.

The phone's LAN configuration includes defining the method for obtaining an IP address. The phone's IP address can be *static* whereby the IP address is manually entered, or *automatic* whereby the IP address is acquired from a DHCP server. For Automatic IP, you can manually define some of the main parameters.

➢ **To define the phone's LAN settings:**

■ **Using the Web:**

1. Access the 'LAN Settings' page (**Configuration** tab > **Network Connections** menu > **Network Settings**).

Figure 13-1: Network Settings Web Fields

2. Configure the LAN settings according to the parameters in the table below, and then click **Submit**.

■   **Using the Configuration File:**

Table 13-1: Network Settings Parameters

Parameter	Description
Note: To add a value to these parameters, enter **network/** followed by the parameter name, equal sign and then the value (e.g. `network/lan_type`=DHCP).	
IP Type **[network/lan_type]**	Defines the IP addressing method: ▪ **[STATIC]** Static IP - Phone's IP address is defined manually ▪ **[DHCP]** Automatic IP DHCP (default) - Phone's IP address is acquired automatically from a DHCP server
network/lan/fixed_ip	This sub-section defines the parameters that are relevant if **lan_type** is configured to "STATIC" or the corresponding **network/lan/dhcp** parameter is set to 1.
IP Address **[network/lan/fixed_ip/ip_address]**	The LAN IP address.
Subnet Mask **[network/lan/fixed_ip/netmask]**	The subnet mask address.
Default Gateway Address **[network/lan/fixed_ip/gateway]**	The IP address of the default gateway.
Domain Name **[network/lan/fixed_ip/domain_name]**	The domain name.
Domain Name Server (DNS)	
Primary DNS **[network/lan/fixed_ip/primary_dns]**	The primary DNS server address.
Secondary DNS **[network/lan/fixed_ip/secondary_dns]**	The secondary DNS server address. The phone connects to this server if the primary DNS server is unavailable.

13.2   Configuring Partial DHCP

Partial DHCP can be configured with the following parameters:

Table 13-2: Partial DHCP Parameters

Partial DHCP	
network/lan/dhcp	This sub-section defines the parameters to configure if **lan_type** is configured to "DHCP".
Domain Name - Manual **[network/lan/dhcp/domain_name/enabled]**	Enables setting the domain name manually. ▪ **[0]** Disable (default) ▪ **[1]** Enable **Note:** If enabled, **network/lan/fixed_ip/domain_name** must also be set.
IP Address - Manual **[network/lan/dhcp/ip_address/enabled]**	Enables setting the IP address manually. ▪ **[0]** Disable (default) ▪ **[1]** Enable **Note:** If enabled, **network/lan/fixed_ip/ip_address** must be set.
Subnet Mask - Manual **[network/lan/dhcp/netmask/enabled]**	Enables setting the network mask manually. ▪ **[0]** Disable (default) ▪ **[1]** Enable **Note:** If enabled, **network/lan/fixed_ip/netmask** must be set.
[network/lan/dhcp/gateway/enabled]	Enables setting the default gateway manually. ▪ **[0]** Disable (default) ▪ **[1]** Enable **Note:** If enabled, **network/lan/fixed_ip/gateway** must be set.
Primary DNS - Manual **[network/lan/dhcp/primary_dns/enabled]**	Enables setting the primary DNS manually. ▪ **[0]** Disable (default) ▪ **[1]** Enable **Note:** If enabled, **network/lan/fixed_ip/primary_dns** must be set.
Secondary DNS - Manual **network/lan/dhcp/secondary_dns/enabled**	Enables setting the secondary DNS manually. ▪ **[0]** Disable (default) ▪ **[1]** Enable **Note:** If enabled, **network/lan/fixed_ip/secondary_dns** must be set.

DHCP-Related Parameters	
network/lan/dhcp/ntp/server_list/enabled	Enables prioritization of the NTP server's information received from the DHCP server (Option fields 42 or 4), over the static configuration (**system/ntp/primary_server_address** and **system/ntp/secondary_server_address**). ▪ **[0]** Disable ▪ **[1]** Enable (default)
network/lan/dhcp/ntp/gmt_offset/enabled	Enables prioritization of the NTP GMT offset information received from the DHCP server (Option field 2), over the static configuration (**system/ntp/gmt_offset**). ▪ **[0]** Disable ▪ **[1]** Enable (default)

Reader's Notes

14   LAN and PC Port Settings

Port settings can be configured using the Web or Configuration File, as described below.

> **Note:** The optional values of the Configuration file parameters are enclosed in square brackets while its corresponding Web values are written outside the square brackets, for example, [1] Enable.

➢ **To define the phone's port settings:**

■ **Using the Web:**

1. Access the 'LAN Settings' page (**Configuration** tab > **Network Connections** menu > **LAN Settings**).

Figure 14-1: Port Mode Web Fields

2. Configure Port Mode according to the parameters in the table below, and then click **Submit**.

■ **Using the Configuration File:**

Table 14-1: Port Settings Parameters

Parameter	Description
LAN Port Mode **[network/lan/port_mode]**	Sets the LAN port mode. Valid values are : [AUTOMATIC] = Auto negotiation. [FULL_10] = 10Mbps + full duplex [FULL_100] = 100Mbps + half duplex [HALF_10] = 10Mbps + full duplex [HALF_100] = 100Mbps + half duplex
PC Port Mode **[network/pc/port_mode]**	Sets the computer port mode. See valid values above.

Reader's Notes

15   VLAN Settings

VLAN settings can be configured using the Web or Configuration File, as described below.

➢ **To configure the phone's VLAN settings:**

■ **Using the Web:**

1. Access the 'Network Settings' page (**Configuration** tab > **Network Connections** menu > **Network Settings**).

Figure 15-1: VLAN Web Fields

▼VLAN Settings	
VLAN Discovery Mode:	Automatic Configuration of VLAN (CDP+LLDP) ▼
Period:	30 Seconds

2. Configure the VLAN settings according to the parameters in the table below, and then click **Submit**.

■ **Using the Configuration File:**

Table 15-1: VLAN Parameters Description

Parameter	Description
VLAN Discovery Mode **[network/lan/vlan/mode]**	Determines the VLAN mode of operation. ▪ **[Disable]** Disable ▪ **[Manual]** Manual Configuration of LAN - Static configuration of VLAN ID and priority ▪ **[CDP]** Automatic Configuration of VLAN - VLAN discovery mechanism based on Cisco Discovery Protocol (CDP) ▪ **[LLDP]** Automatic Configuration of VLAN - VLAN discovery mechanism based on LLDP. ▪ **[CDP_LLDP]** Automatic Configuration of VLAN (default) - VLAN discovery mechanism based on LLDP and Cisco Discovery Protocol (CDP). LLDP protocol is with higher priority.
Period **[network/lan/vlan/period]**	The time period in seconds between discovery messages when configured to CDP, LLDP or CDP and LLDP. The default value is 30.
VLAN ID **[network/lan/vlan/id]**	The VLAN ID. The valid range is 0 to 4096. The default VLAN ID is 0.
VLAN Priority **[network/lan/vlan/priority]**	The priority of traffic pertaining to this VLAN. The valid range is 0 to 7 (where 7 is the highest priority). The default VLAN priority is 0.

Reader's Notes

16 Enabling Telnet Access
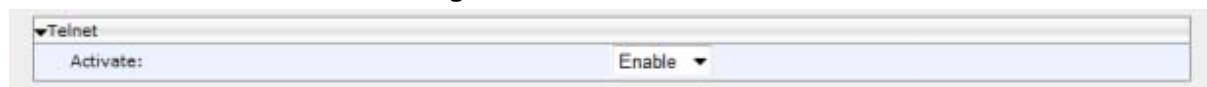
Telnet access can be enabled using the Web or Configuration File, as described below.

➢ **To enable Telnet:**

■ **Using the Web:**

1. Access the 'Telnet' page (**Management** tab > **Remote Management** menu > **Telnet**).

Figure 16-1: Telnet Web Field

2. Enable Telnet according to the parameter in the table below, and then click **Submit**.

■ **Using the Configuration File:**

Table 16-1: Telnet Parameters

Parameter	Description
Note: To add a value to these parameters, enter **management/** followed by the parameter name, equal sign and then the value (e.g. `management/telnet/enabled=0`).	
Activate **[management/telnet/enabled]**	Enables telnet access to the phone. ▪ **[0]** Disable (default) ▪ **[1]** Enable The user name and password for telnet access are according to the parameters: **system/user_name** and **system/password**.

Reader's Notes

AudioCodes

Part V

VoIP Settings

Reader's Notes

17   SIP Settings

The following can be configured using the Web or Configuration File, as described below.

- General
- Proxy and Registration
- SIP Timers
- SIP QoS

17.1   Configuring General SIP Settings

SIP General settings can be configured using the Web or Configuration File, as described below.

➢ **To configure the phone's general SIP settings:**

- **Using the Web:**
    1. Access the 'Signaling Protocol' page (**Configuration** tab > **Voice Over IP** menu > **Signaling Protocols**).

Figure 17-1: SIP General Web Fields

    2. Configure the General settings according to the parameters in the table below, and then click **Submit**.

■ **Using the Configuration File:**

Table 17-1: SIP General Parameters

Parameter	Description
SIP Transport Protocol **[voip/signalling/sip/transport_protocol]**	Determines the transport layer for outgoing SIP calls initiated by the phone. ▪ **[UDP]** UDP (default) ▪ **[TCP]** TCP ▪ **[TLS]** TLS
TLS Port **[voip/signalling/sip/tls_port]**	Defines the local TLS SIP port for SIP messages. The valid range is 1024 to 65535. The default value is 5061.
/voip/signalling/sip/enable_sips	Relevant for TLS only, if enabled, the request URI prefix will be "sips:" otherwise, the prefix will be "sip:"
/voip/signalling/sip/subs_no_notify_timer	Indicates the maximum time (in milliseconds) that a subscription waits from receiving 2xx response for a SUBSCRIBE request, until receiving the first NOTIFY request. If the timer expires, the subscription will be terminated.
SIP Local Port **[voip/signalling/sip/port]**	Defines the local SIP port (UDP or TCP) for SIP messages. The valid range is 1024 to 65535. The default value is 5060.
Gateway Name **[voip/signalling/sip/proxy_gateway]**	Assigns a name to the phone. The name is used as the host part of the SIP URI in the From header. **Notes:** ▪ Ensure that the name you choose is the one with which the Proxy is configured to identify the phone. ▪ If not specified, the phone's IP address is used (default).
PRACK Mode **[voip/signalling/sip/prack/enabled]**	Determines whether the phone sends PRACK (Provisional Acknowledgment) messages upon receipt of 1xx SIP reliable responses. ▪ **[0]** Disable ▪ **[1]** Enable (default)

Parameter	Description
Enable RPORT **[voip/signalling/sip/rport/enabled]**	Determines whether the phone adds the 'rport' parameter to the relevant SIP message (in the SIP Via header). ▪ **[0]** Disable (default) ▪ **[1]** Enable
Include PTIME in SDP **[voip/signalling/sip/sdp_include_ptime]**	Determines whether the phone adds the PTIME parameter to the SDP message body. ▪ **[0]** Disable (default) ▪ **[1]** Enable
Enable Keep Alive using OPTIONS **[voip/signalling/sip/keepalive_options/enabled]**	Determines whether keep-alive is performed using SIP OPTIONS messages sent to the Proxy. ▪ **[0]** Disable (default) ▪ **[1]** Enable
Keep Alive Period **[voip/signalling/sip/keepalive_options/timeout]**	Defines the Proxy keep-alive time interval (in seconds) between Keep-Alive messages. The valid range is 0 to 86400. The default value is 300.
Connect Media on 180 Response **[voip/signalling/sip/connect_media_on_180]**	Determines whether the media is connected upon receipt of SIP 180, 183, or 200 messages. When the parameter is disabled, media is connected upon receipt of 183 and 200 messages only. ▪ **[0]** Disable (default) ▪ **[1]** Enable
Block Caller ID on Outgoing Calls **[voip/signalling/sip/block_callerid_on_outgoing_calls]**	When enabled, the outgoing INVITE message is sent with an anonymous From header and P-Asserted-Identity header. ▪ **[0]** Disable (default) ▪ **[1]** Enable For example: ▪ FROM header contains anonymous URI: *From: "Anonymous" sip:anonymous@anonymous.invalid* ▪ P-Asserted-Identity header: *P-Asserted-Identity:* "1001" 1115551001@proxy.net

Parameter	Description
Incoming Anonymous Call Blocking **[voip/signalling/sip/anonymous_calls_blocking]**	When enabled, incoming INVITE messages with anonymous From header are rejected. ▪ **[0]** Disable (default) ▪ **[1]** Enable For example: *From:"Anonymous"<sip:anonymous@anonymous.invalid>* The phone responds with a SIP 403 "Forbidden" response.
[voip/signalling/sip/auth_retries]	Defines the number of times authenticated register messages are re-sent if 401 or 407 SIP responses with a different "nonce" are received. The valid range is 0 to 100. The default value is 4.
[voip/signalling/sip/display_name_in_registration_msg/enabled]	Sets the Display Name in the "To" and "From" fields of the SIP REGISTER message. ▪ **[0]** Disable (default) ▪ **[1]** Enable
voip/signalling/sip/semi_transfer_with_no_cancel/enabled	Determines whether semi-attendant transfer is performed without sending the SIP CANCEL message to the remote side. ▪ **[0]** Disable (default) ▪ **[1]** Enable **Notes:** ▪ In this flow ("with_no_cancel"), the Transferor's User Agent continues the transfer as an attended transfer even after the Transferor hangs up. This is the recommended flow defined by http://tools.ietf.org/html/draft-ietf-sipping-cc-transfer-03. ▪ Existing / current behavior is retained for backward compatibility (disabled by default)

17.2   Proxy and Registration

This section describes the process for configuring Proxy and Registration settings.

17.2.1   Configuring General Proxy and Registration Settings

Proxy and Registration settings can be configured using the Web or Configuration File, as described below.

➤ **To configure the phone's Proxy and Registration settings:**

■ **Using the Web:**

1. Access the 'Signaling Protocol' page (**Configuration** tab > **Voice Over IP** menu > **Signaling Protocols**).

Figure 17-2: SIP Proxy and Registrar Web Fields

2. Configure Proxy and Registration according to the parameters in the table below, and then click **Submit**.

■ **Using the Configuration File:**

Table 17-2: Proxy and Registrar Parameters

Parameter	Description
Use SIP Proxy **[voip/signalling/sip/use_proxy]**	Determines whether to use a SIP Proxy server. ▪ **[0]** Disable (default) ▪ **[1]** Enable
voip/signalling/sip/proxy_address	The IP address or host name of the SIP proxy server. The default value is 0.0.0.0.
Proxy Port **[voip/signalling/sip/proxy_port]**	The UDP or TCP port of the SIP proxy server. The valid range is 1024 to 65535. The default value is 5060.
Enable Registrar Keep Alive **[voip/signalling/sip/registrar_ka/enabled]**	Determines whether to use the registration keep-alive mechanism based on SIP OPTION messages. ▪ **[0]** Disable (default) ▪ **[1]** Enable **Notes:** ▪ If there is no response from the server, the timeout for re-registering is automatically reduced to a user-defined value (**voip/signalling/sip/registration_failed_timeout**) ▪ When the phone re-registers, the keep-alive messages are re-sent periodically.
Registrar Keep Alive Period **voip/signalling/sip/registrar_ka/timeout**	Defines the registration keep-alive time interval (in seconds) between Keep-Alive messages. The valid range is 40 to 65536. The default value is 60.
Maximum Number of Authentication Retries **voip/signalling/sip/proxy_timeout**	The SIP proxy server registration timeout (in seconds). The valid range is 0 to 86400. The default value is 3600.
Registration Failed Expires **voip/signalling/sip/registration_failed_timeout**	If registration fails, this parameter determines the interval between the register messages periodically sent until successful registration. The valid range is 1 to 86400. The default value is 60.
Use SIP Registrar **voip/signalling/sip/sip_registrar/enabled**	Determines whether the phone registers to a separate SIP Registrar server. ▪ **[0]** Disable (default) ▪ **[1]** Enable

Parameter	Description
Use SIP Proxy IP and Port for Registration **voip/signalling/sip/use_proxy_ip_port_for_registrar**	Determines whether to use the SIP proxy's IP address and port for registration. When enabled, there is no need to configure the address of the registrar separately. ▪ **[0]** Disable (default) ▪ **[1]** Enable
Registrar IP Address or Host Name **voip/signalling/sip/sip_registrar/addr**	The IP address or host name of the Registrar server. The default value is 0.0.0.0.
Registrar Port **voip/signalling/sip/sip_registrar/port**	The UDP or TCP port of the Registrar server. The valid range is 1024 to 65535. The default value is 5060.
Use SIP Outbound Proxy **[voip/signalling/sip/sip_outbound_proxy/enabled]**	Determines whether an outbound SIP proxy server is used (all SIP messages are sent to this server as the first hop). ▪ **[0]** Disable (default) ▪ **[1]** Enable
Outbound Proxy IP Address or Host Name **[voip/signalling/sip/sip_outbound_proxy/addr]**	The IP address of the outbound proxy. If this parameter is set, all outgoing messages (including Registration messages) are sent to this Proxy according to the Stack behavior. The default value is 0.0.0.0.
Outbound Proxy Port **[voip/signalling/sip/sip_outbound_proxy/port]**	The port on which the outbound proxy listens. The valid range is 1024 to 65535. The default value is 5060.

17.2.2 Configuring Proxy Redundancy

The Redundant Proxy feature allows the configuration of a backup SIP proxy server to increase QoS stability. Once this feature is enabled, the phone identifies cases where the primary proxy does not respond to SIP signaling messages. In these scenarios, the phone registers to the redundant proxy and the phone seamlessly continues normal functionality, without the user noticing any connectivity failure or malfunction with the primary proxy.

The Redundant Proxy feature can operate in one of the following modes:

■ **Asymmetric mode**: The primary proxy is assigned a higher priority for registration than the redundant proxy. Once the phone is registered to the primary proxy, it sends keep-alive messages (using SIP OPTIONS messages) to the primary proxy. If the primary proxy does not respond, the phone registers to the redundant proxy, but continues sending keep-alive messages to the primary proxy. **If the primary proxy responds to these keep-alive messages, the phone re-registers to the primary proxy.**

■ **Symmetric mode:** Both proxies are assigned the same priority for registration. Once the phone is registered to a proxy, it sends keep-alive messages to this proxy. The phone switches proxies only once the proxy to which it has registered, does not respond.

For more information see the **[voip/signalling/sip/redundant_proxy/symmetric_mode]** description in the SIP Proxy Server Redundancy Parameters table below.

Proxy Redundancy can be configured using the Web or Configuration file.

➢ **To configure Proxy Redundancy:**

■ **Using the Web:**

1. Access the 'Signaling Protocol' page (**Configuration** tab > **Voice Over IP** menu > **Signaling Protocols**).

Figure 17-3: Proxy Redundancy

2. Configure the SIP Redundancy parameters according to the table below, and then click **Submit**.

■   **Using the Configuration file:**

Table 17-3: SIP Proxy Server Redundancy Parameters

Parameter	Description
Use Redundant Proxy **[voip/signalling/sip/redundant_proxy/enabled]**	Enables the redundant proxy mechanism. ▪ **[0]** Disable (default) - Phone doesn't use redundant proxy (default). ▪ **[1] Enable** - Phone registered to redundant proxy if the primary proxy does not respond to SIP signaling messages.
Redundant Proxy Address **[voip/signalling/sip/redundant_proxy/address]**	The IP address or host name of the redundant proxy. The default value is 0.0.0.0. **Note:** This parameter is applicable only if the parameter **use_redundant_proxy** is set to 1.
Redundant Proxy Port **voip/signalling/sip/redundant_proxy/port**	The UDP or TCP port of the redundant proxy server. The valid range is 1024 to 65535. The default value is 5060. **Note:** This parameter is applicable only if the parameter **use_redundant_proxy** is set to 1.
Redundant Proxy Keep Alive Period **voip/signalling/sip/redundant_proxy/keepalive_period**	Defines the interval in seconds for sending keep-alive messages to the proxy. The valid range is 0 to 300. The default value is 60. **Note**: This parameter is applicable only if the parameter **use_redundant_proxy** is set to 1.
Switch back to Primary SIP proxy when available **[voip/signalling/sip/redundant_proxy/symmetric_mode]**	Determines the proxy redundancy mode. [0]- Asymmetric mode. (default) [1] - Symmetric mode. The Redundant Proxy feature allows the configuration of a backup SIP proxy server to increase QoS stability. Once this feature is enabled, the phone identifies cases where the primary proxy does not respond to SIP signaling messages. In these scenarios, the phone registers to the redundant proxy and the phone seamlessly continues normal functionality, without the user noticing any connectivity failure or malfunction with the primary proxy. The Redundant Proxy feature includes two operational modes: ▪ Asymmetric mode: the primary proxy is assigned a higher priority for registration than the redundant proxy.

Parameter	Description
	In the Asymmetric mode, once the phone is registered to the primary proxy, it sends keep-alive messages (using SIP OPTIONS messages) to the primary proxy. If the primary proxy does not respond, the phone registers to the redundant proxy, but continues sending keep-alive messages to the primary proxy. If the primary proxy responds to these keep-alive messages, the phone re-registers to the primary proxy. Therefore, the phone assigns the primary proxy a higher priority for registration. ▪ Symmetric mode: both proxies are assigned the same priority for registration. In the Symmetric mode, once the phone is registered to a proxy, it sends keep-alive messages to this proxy. The phone switches proxies only once the proxy to which it has registered does not respond. Therefore, the phone assigns both proxies the same priority for registration In both modes, the following applies: If the phone is not registered (i.e., if the proxy server¬–redundant or primary–to which the phone currently tries to register does not respond), the phone attempts to register to an alternative proxy. These attempts continue until the phone successfully registers. If this feature is enabled and the user reboots the phone, the phone registers to the last proxy to which it was trying to register, and not necessarily to the primary proxy. **Note:** This parameter is applicable only if the parameter use_redundant_proxy is set to 1.

17.3   Configuring SIP Timers

SIP Timers can be configured using the Web or Configuration File, as described below.

➢ **To configure the phone's SIP timer settings:**

■ **Using the Web:**

   1. Access the 'Signaling Protocol' page (**Configuration** tab > **Voice Over IP** menu > **Signaling Protocols**).

Figure 17-4: SIP Timers

SIP Timers	
Retransmission Timer T1:	500
Retransmission Timer T2:	4000
Retransmission Timer T4:	5000
INVITE Timer:	32000
Session-Expires:	1800
Min-SE:	90

   2. Configure the SIP Timer parameters according to the table below, and then click **Submit**.

■ **Using the Configuration file:**

Table 17-4: SIP Timers Parameters

Parameter	Description
Retransmission Timer T1 **[voip/signalling/sip/sip_t1]**	The time interval (in msec) between the first transmission of a SIP message and the first retransmission of the same message (according to RFC 3261). The valid range is 100 to 60000. The default value is 500. **Note:** The time interval between subsequent retransmissions of the same SIP message starts with SipT1Rtx and is multiplied by two until SipT2Rtx. For example (assuming that SipT1Rtx = 500 and SipT2Rtx = 4000): ▪ The first retransmission is sent after 500 msec. ▪ The second retransmission is sent after 1000 (2*500) msec. ▪ The third retransmission is sent after 2000 (2*1000) msec. ▪ The fourth retransmission and subsequent retransmissions until SIPMaxRtx are sent after 4000 (2*2000) msec..
Retransmission Timer T2 **[voip/signalling/sip/sip_t2]**	The maximum interval (in msec) between retransmissions of SIP messages (according to RFC 3261). The valid range is 4000 to 60000. The default value is 4000. **Note:** The time interval between subsequent retransmissions of the same SIP message starts with SipT1Rtx and is multiplied by two until SipT2Rtx.
Retransmission Timer T4 **[voip/signalling/sip/sip_t4]**	The SIP T4 retransmission timer according to RFC 3261. The valid range is 5000 to 60000. The default value is 5000.
INVITE Timer **[voip/signalling/sip/sip_invite_timer]**	The SIP INVITE timer according to RFC 3261. The valid range is 0 to 65535. The default value is 32000.
Session-Expires **[voip/signalling/sip/session_timer]**	The time (in seconds) at which an element considers the call timed out if no successful INVITE transaction occurs beforehand. This value is inserted into every INVITE in the Session-Expires header unless it is configured to 0. If the timer option tag is not part of the supported list, the sessionExpires value is ignored. The valid range is 0 to 65535. The default value is 1800.
Min-SE **[voip/signalling/sip/min_session_interval]**	The minimum value for the session interval that the application is willing to accept. The valid range is 0 to 65535. The default value is 90.

17.4   Configuring SIP QoS
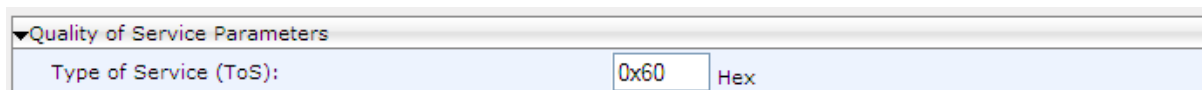
SIP Quality of Service (QoS) can be configured using the Web or Configuration File, as described below.

➢ **To configure the phone's SIP QoS:**

■ **Using the Web:**

1. Access the 'Signaling Protocol' page (**Configuration** tab > **Voice Over IP** menu > **Signaling Protocols**).

Figure 17-5: Quality of Service Page

2. Configure the SIP Quality of Service parameters according to the table below, and then click **Submit**.

■ **Using the Configuration File:**

Table 17-5: SIP QoS Parameters

Parameter	Description
Type of Service (ToS) **[voip/signalling/sip/tos]**	QoS in hexadecimal format. This is a part of the IP header that defines the type of routing service to tag outgoing signalling packets originated from the phone. It informs routers that this packet must receive a specific QoS. The default value is 0x60. Values can be set in decimal (e.g. 96) or hexadecimal (e.g. 0x60).

For information on Configuring RTP QoS, see Section 19.3 on page 119.

17.5 Configuring SIP Reject Code

Reject Code can be configured using the Web or Configuration File, as described below.

➢ **To configure Reject Code:**

■ **Using the Web:**

1. Access the 'Services' page (**Configuration** tab > **Voice Over IP** menu > **Services** > **General Parameters**).

Figure 17-6: Reject Code Web Field

Reject Code:	603 ▼

2. Configure the Reject Code parameters according to the table below, and then click **Submit**.

■ **Using the Configuration File:**

Table 17-6: Reject Code Parameter

Parameter	Description
/voip/services/reject_code	Configures the reject code that the IP Phone will send when pressing the **Reject** softkey or while DND is activated. Valid values are: **[CODE_603]** **[CODE_486]**

18   Dialing Settings

Dialing Settings can be configured using the Web or Configuration File, as described below.

18.1   Configuring General Dialing Settings

General Dialing settings can be configured using the Web or Configuration File, as described below.

➢ **To define the dialing parameters:**

■ **Using the Web:**

1.   Access the 'Dialing' page (**Configuration** tab > **Voice Over IP** menu > **Dialing**).

Figure 18-1: General Dialing Web Fields

Dialing Timeout:	5	Seconds
Phone Number Length:	19	Digits
Enable Dialing Complete Key:	Enable	
Dialing Complete Key:	#	

2.   Configure Dialing options according to the parameters in the table below, and then click **Submit**.

■ **Using the Configuration File:**

Table 18-1: Dialing Parameters

Parameter	Description
Dialing Timeout **[voip/dialing/timeout]**	The duration (in seconds) of allowed inactivity between dialled digits. When you work with a proxy, the number you have dialled before the dialing process has timed out is sent to the proxy as the user ID to be called. This is useful for calling a remote party without creating a speed dial entry (assuming the remote party is registered with the proxy). The valid range is 0 to 10. The default value is 5.
Phone Number Length **[voip/dialing/phone_number_max_size]**	The maximum length of shortcut numbers that you can enter and the maximum number of digits that you can dial The valid range is 3 to 32. The default value is 32.
Enable Dialing Complete Key **[voip/dialing/dial_complete_key/enabled]**	Enables the feature for defining a key to indicate that dialing has completed. Pressing the Dialing Complete key (defined below) forces the phone to make a call to the dialled digits even if there is no match in the dial plan or digit map. ▪ **[0]** Disable ▪ **[1]** Enable (default) **Note:** This parameter is available only if the parameter **voip/dialing/dial_complete_key/enabled** is set to 1.
Dialing Complete Key **[voip/dialing/dial_complete_key/key]**	Defines the Dialing Complete key. The valid value is a single character. The default value is the pound (#) key.
No Answer Call Timeout **[voip/dialing/unanswered_call_timeout]**	Timeout before the phone automatically sends a Cancel message. When the phone makes a call and the other side doesn't answer, the phone sends a Cancel after this timeout The valid range is 1 to 300. The default value is 60.
[voip/dialing/on_hook_dialing]	Defines the dialing mode when phone is on hook and no audio device is selected (when user enters digits on idle state). Valid values are: **[Disable]** = Ignore digits press. In order to initiate a call the user will have to select audio device by pressing speaker or headset keys or by picking headset. **[Open_default_audio_device]=** default behavior – start dialing via default audio device (usually speaker) activated. **[Off_line_dialing]** = don`t activate the default audio device until pressing "dial" , DTMF tones will not be heard and dialing related features (such as "dialing timeout" , "dial complete key" , and more) will be disabled.
[voip/dialing/allow_calling_self_extension]	If disabled (default), calling the self-number (user ID) will be blocked. If enabled, the phone will send the invite although it is for its own extension. (In some proxies this is how you access voice mail).
[voip/dialing/speed_dial/double_press/enabled]	Relevant for 310HD only, if enabled, the first speed dial press will display the number and only the second press will dial. If disabled, the first press will dial.

18.2   Tones

Tones settings can be configured using the Web or Configuration File, as described below.

➢   **To configure the dial tones:**

■   **Using the Web:**

1.   Access the 'Dialing' page (**Configuration** tab > **Voice Over IP** menu > **Dialing**).

Figure 18-2: Tones Web Fields in Dialing Page

Dial Tone Timeout:	30	Seconds
Reorder Tone Timeout:	40	Seconds
No Answer Call Timeout:	60	Seconds
Howler Tone Timeout:	120	Seconds
Secondary Dial Tone:	Enable	
Secondary Dial Tone Key:	9	

2.   Access the 'Services' page (**Configuration** tab > **Voice Over IP** menu > **Services**).

Figure 18-3: Tones Web Fields in Services Page

Stutter Tone Duration:	2500	msec
Out of Service Behavior:	Reorder Tone	
Automatic Disconnect:	Enable	

3.   Configure Tones options according to the parameters in the table below, and then click **Submit**.

■   **Using the Configuration File:**

Table 18-2: Dial Tones Parameters

Parameter	Description
Dial Tone Timeout **[voip/dialing/dialtone_timeout]**	Defines the maximum duration of the dial tone (in seconds) after which the dial tone stops and a reorder tone is played. The valid range is 1 to 300. The default value is 30.
Reorder Tone Timeout **[voip/dialing/warning_tone_timeout]**	Defines the maximum duration of the reorder tone (in seconds) after which the reorder tone stops and a howler tone is played. The valid range is 1 to 300. The default value is 40.
Howler Tone Timeout **[voip/dialing/offhook_tone_timeout]**	Defines the duration (in seconds) of the howler tone. If the limit is exceeded, the howler tone stops. The howler tone indicates that the phone has been left in an off-hook state. The valid range is 1 to 300. The default value is 120.

Parameter	Description
Secondary Dial Tone **[voip/dialing/secondary_dial_tone/enabled]**	Enables the secondary dial tone. ▪ **[0]** Disable - Phone doesn't use secondary dial tone. ▪ **[1]** Enable (default) - Phone plays secondary dial tone if the secondary dial tone key is pressed (first digit).
Secondary Dial Tone Key **[voip/dialing/secondary_dial_tone/key_sequence]**	Defines the secondary dial tone is played if this is the first key pressed. The valid range is 0 to 9. The default value is 9. **Note:** This parameter is available only if the parameter **voip/dialing/secondary_dial_tone/enabled** is set to 1.
Out of Service Behavior **[voip/services/out_of_service_behavior]**	Determines whether a reorder tone is played instead of a dial tone if you configured a Registrar IP address and the registration failed. ▪ **[NONE]** No Tone ▪ **[REORDER_TONE]** Reorder Tone (default)
Stutter Tone Duration **[voip/services/msg_waiting/stutter_tone_duration]**	Defines the duration for which a stutter tone is played when you have unheard messages. The valid range is 1000 to 60000. The default value is 2500.
Automatic Disconnect **[voip/dialing/automatic_disconnect]**	Determines whether the phone automatically goes idle (i.e. on-hook) when the last remaining call is disconnected. This is only relevant when the speaker or headset is used. ▪ **[0]** Disable ▪ **[1]** Enable(default)

18.2.1   Uploading Ring Tones

New Ring Tones can be uploaded using the Web or Configuration File, as described below.

> **Notes:**
>
> - The ring tone file must be in WAV file format (A/Mu-Law, 8-kHz audio sample rate and 8-bit audio sample size or PMC 16-kHz audio sample rate and 16-bit audio sample size, Intel PCM encoding).
> - If you want the phone to use an uploaded ring tone, you need to use the phone's LCD screen to select it (refer to the phone's *User's Manual*).

➢ **To upload a ring tone:**

◼ **Using the Web:**

   1. Access the 'Tones' page (**Configuration** tab > **Personal Settings** menu > **Tones**).

Figure 18-4: Upload Ringing Tones Web Fields

   2. In the 'Ringing Tone Name' field, enter the name of the ring tone file that you want to upload. If you do not enter a name, the phone assigns the tone's file name (without the *.wav* file extension) as the name of the tone.

   3. Click the **Browse** button, navigate to the folder in which the ring tone file is located, select the file, and then click **Open**; the file name and path is displayed in the 'File Location' field.

   4. Click **Submit**; the file is loaded to the phone and displayed in the Ring Tone list.

➢ **To delete Ring Tones:**

- Deleting selected ring tones: select the 'Delete' check boxes corresponding to the ring tone that you want to delete, and then click **Submit**.

■ **Using the Configuration File:**

Table 18-3: Ring Tone Parameters

Parameter	Description
Ringing Tone Name File Location **[provisioning/ring_tone_uri]**	The URI for retrieving the ring tones file. The ring tones can be compressed to *.zip or *.tgz files and provided to the phone during provisioning. For example: **provisioning/ring_tone_uri=tones.tgz** **Notes:** ▪ The ringtone file is downloaded only after boot up, and not periodically. ▪ If the tones file is new, the phone updates the information, but does not reboot.

18.2.2 Regional Settings for Call Progress Tones

You can suite your phone's call progress tones to the location in which the phone is located. In addition, instead of using the default ring tone, you can upload a different ring tone file and use that ring tone for indicating incoming calls. This ring tone can only be selected using the phones LCD interface.

Follow the procedure below for selecting the region in which your phone is located. This is important for suiting your phone for the call progress tones of the country in which the phone is located.

➢ **To select the geographical location of your phone:**

■ **Using the Web:**

1. Access the 'Tones' page (**Configuration** tab > **Personal Settings** menu > **Tones**).

Figure 18-5: Tones Web Fields

2. From the 'Current Location' drop-down list, select the country in which your phone is located.
3. Click **Submit**.

■ **Using the Configuration File:**

Table 18-4: Regional Parameters

Parameter	Description
Current Location **[voip/regional_settings/selected_country]**	Defines the country in which your phone is located. The behavior and parameters of analog telephones lines vary between countries. The set of Call Progress Tones are all location-specific. The phone automatically selects the correct regional settings according to this setting. Supported countries: ▪ **[Israel]** Israel ▪ **[China]** China ▪ **[France]** France ▪ **[Germany]** Germany ▪ **[Netherlands]** Netherlands ▪ **[UK]** UK ▪ **[Brazil]** Brazil ▪ **[Italy]** Italy ▪ **[Argentina]** Argentina ▪ **[Portugal]** Portugal ▪ **[Russia]** Russia ▪ **[Australia]** Australia ▪ **[USA]** USA
voip/regional_settings/use_config_file_values	Enables the user-defined CPT. When this parameter is enabled, the **selected_country** parameter is not relevant and the below Call Progress Tones values can be determined by the user. ▪ **[0]** - Disable (default) ▪ **[1]** - Enable
Call Progress Tones (CPT) **Note:** Up to 10 CPT's can be configured (**voip/regional_settings/call_progress_tones/0…9**).	
voip/regional_settings/call_progress_tones/%d/enabled	Enables the specific CPT. ▪ **[0]** - Disable ▪ **[1]** - Enable
voip/regional_settings/call_progress_tones/%d/name	Defines the name of the CPT.
voip/regional_settings/call_progress_tones/%d/cadence	Defines the cadence type of the tone. ▪ **[0]** - Continuous signal ▪ **[1]** - Cadence signal ▪ **[2]** - Burst signal
voip/regional_settings/call_progress_tones/%d/frequency_a	Defines the low frequency (in Hz) of the tone. The valid value range is 300 to 1980 Hz, in steps of 1 Hz. Unused frequencies must be set to zero.
voip/regional_settings/call_progress_tones/%d/frequency_b	Defines the high frequency (in Hz) of the tone. The valid value range is 300 to 3000 Hz, in steps of 1 Hz. Unused frequencies must be set to zero.

Parameter	Description
voip/regional_settings/call_progress_tones/%d/frequency_a_level	Output level of the low frequency tone (in -dBm) in Call Progress generation. The valid range is 0 to 63, where 63 is mute.
voip/regional_settings/call_progress_tones/%d/frequency_b_level	Output level of the low frequency tone (in -dBm) in Call Progress generation. The valid range is 0 to 63, where 63 is mute.
voip/regional_settings/call_progress_tones/%d/tone_on_0	tone_on_0 to tone_on_3. If the signal is Cadence or Burst, then this value represents the on duration. If a Continuous tone, then this value represents the minimum detection time. The units are in 10 msec. The valid range is 0 to 10000.
voip/regional_settings/call_progress_tones/%d/tone_off_0	tone_off_0 to tone_on_3. If the signal is Cadence, then this value represents the off duration. The units are in 10 msec. If it is not used, then set it to zero. If the signal is Burst, only tone_off 0 is relevant. It represents the off time that is required from the end of the signal to the detection time. The valid range is 0 to 10000.

18.3   Configuring Default Audio Device
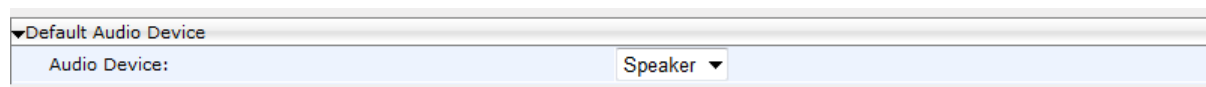
Default Audio Device Tones settings can be configured using the Web or Configuration File, as described below.

➢ **To configure default Audio Device:**

■ **Using the Web:**

    1. Access the 'Dialing' page (**Configuration** tab > **Voice Over IP** menu > **Dialing**).

Figure 18-6: Default Audio Device Web Field

```
▼Default Audio Device
  Audio Device:                    Speaker ▼
```

    2. Configure the parameter according to the table below and then click **Submit**.

■ **Using the Configuration file:**

Table 18-5: Audio Device Parameter

Parameter	Description
Audio Device **[voip/answer_device]**	Sets the default audio device to answer or initiate a new call when no explicit audio device is set. For example: ▪ When pressing ANS SK. ▪ When initiating a call by speed dial key, call history or phone directory. ▪ Answering talk event or auto-answer. ▪ When starting to dial in "on hook" mode. Valid values are: ▪ [SPEAKER] ▪ [HEADSET]

18.4   Configuring DTMF

DTMF can be configured using the Web or Configuration File, as described below.

➤ **To configure DTMF:**

■ **Using the Web:**

1. Access the 'Dialing' page (**Configuration** tab > **Voice Over IP** menu > **Dialing**).

Figure 18-7: DTMF Transport Mode Web Field

DTMF Transport Mode:	RFC 2833 ▾

2. Configure the parameter according to the table below and then click **Submit**.

■ **Using the Configuration file:**

Table 18-6: DTMF Description

Parameter	Description
DTMF Transport Mode **[voip/media/out_of_band_dtmf]**	DTMF transport mode. ▪ **[INBAND]** Inband ▪ **[RFC2833]** RFC 2833 (default) ▪ **[VIA_SIP]** Via SIP

18.5   Configuring Digit Maps and Dial Plans

Digit maps and Dial plans can be configured using the Web or Configuration File, as described below.

➢ **To configure digit map and dial plan:**

■ **Using the Web:**

1. Access the 'Dialing' page (**Configuration** tab > **Voice Over IP** menu > **Dialing**).

Figure 18-8: Digit Map and Dial Plan Web Fields

| Digit Map: | |
| Dial Plan: | |

2. Configure the parameters according to the table below, and then click **Submit**.

■ **Using the Configuration file:**

Table 18-7: Digit Map and Dial Plan Parameters

Parameter	Description

Digit Map
[voip/signalling/sip/digit_map]
	Enables the administrator to predefine possible formats (or patterns) for the dialed number. A match to one of the defined patterns terminates the dialed number.
	The valid value can be up to 256 characters.
	There are two main formats for the digit map configuration. The formats are distinguished by the separator ';' or '|'.
	
	▪ **Using '|' separator:** The following constructs can be used in each numbering scheme:
	  ✓ **Digit:** A digit from "0" to "9".
	  ✓ **DTMF:** A digit, or one of the symbols "A", "B", "C", "D", "#", or "*". Extensions may be defined.
	  ✓ **Wildcard:** The symbol "x" which matches any digit ("0" to "9").
	  ✓ *** Range:** One or more DTMF symbols enclosed between square brackets ("[" and "]").
	  ✓ **Sub range:** Two digits separated by hyphen ("-") which matches any digit between and including the two. The subrange construct can only be used inside a range construct, i.e., between "[" and "]".
	  ✓ **Position:** A period (".") which matches an arbitrary number, including zero, of occurrences of the preceding construct.
	For example: [2-9]11|0|100|101|011xxx.|9011xxx.|1[2-9]xxxxxxxxx|91[2-9]xxxxxxxxx|9[2-9]xxxxxx|*xx|[8]xxxx|[2-7]xxx
	This example includes the following rules:
	  ✓ **[2-9]11:** 911 rule: 211, 311, 411, 511, 611, 711, 811, 911 are dialed immediately
	  ✓ **0:** Local operator rule: After dialing "0" the phone waits T seconds and then completes the call automatically
	  ✓ **100:** Auto-attendant default extension
	  ✓ **101:** Voicemail default extension
	  ✓ **011xxx.:** International rule without prefix

Parameter	Description
	✓ **9011xxx.:** International rule with prefix ✓ **1[2-9]xxxxxxxxx:** LD rule without prefix ✓ **91[2-9]xxxxxxxxx:** LD rule with prefix ✓ **9[2-9]xxxxxx:** Local call with prefix ✓ ***xx:** 2-digit star codes ✓ **[1-7]xx:** A regular 3 digit extension that does not start with 9 or 8 is dialed immediately ✓ **[2-7]xx:** A regular 3 digit extension that does not start with 9 or 8 or 1 is dialed immediately ✓ **[2-7]xxx:** A regular 4 digit extension that does not start with 9 or 8 or 1 is dialed immediately ✓ **[8]xxx:** A 3 digit extension prefixed with an 8 (routes calls directly to voicemail of extension xxx) ✓ **[8]xxxx:** A 4 digit extension prefixed with an 8 (routes calls directly to voicemail of extension xxxx) ✓ **T**: Refers to the **Dialing Timeout.** ▪ **Using ';' separator:** An 'x' in the pattern indicates any digit. ';' separates between patterns. For example: '10x;05xxxxxxxx;4xxx'. In this example, three patterns are defined. A number that starts with 10 is terminated after the third digit, and so on. If the user dials a number that does not match any pattern, the number is terminated using the timeout or when the user presses the pound ('#') key.
voip/signalling/sip/number_rules	This parameter works in conjunction with the parameter **voip/signalling/sip/digit_map** and enables translation of specific patterns to specific SIP destination addresses. An 'x' represents any dialed digit. Each backslash at the right side of the '=' represents one of the dialed digits. Rules are separated by the character ';'. The valid value can be up to 256 characters. For example: '4xxx=Line_\\\@10.1.2.3' This rule issues a call to 10.1.2.3 with the SIP ID of Line_ followed by the last three digits of the dialed number.

Reader's Notes

19 Media Settings

The procedures for configuring media settings are described below.

19.1 Configuring Media Streaming

The Configuring Media Streaming feature can be configured using the Configuration File parameters as described in the table below.

Table 19-1: Media Streaming Parameters

Parameter	Description
voip/media/rtp_mute_on_hold	Mute sending RTP packets to remote in HOLD state. • **[0]** - Disabled. RTP packets are sent to remote end when in HOLD state. • **[1]** - Enabled (default). RTP packets are not sent to remote end when in HOLD state.
voip/media/allow_multiple_rtp	Defines whether to allow multiple RTP streams from different remote ends to be played toward the phone in a single call. • **[0]** Disable (default) • **[1]** Enable
voip/media/ignore_rfc_2833_packets	Defines whether to ignore playing DTMF when RFC2833 arrives from the network. • **[0]** Disable • **[1]** Enable (default)
/voip/media/broken_connection_detection	If enabled an active call will be automatically disconnected if no RTP packet is received within pre-defined time.
/voip/media/broken_connection_timeout	If no RTP packet arrives for an active call within this timeout (in seconds), the connection will be considered broken and the call will be disconnected.

19.2 Configuring RTP Port Range and Payload Type

RTP Port Range and Payload Type can be configured using the Web or Configuration File, as described below.

➢ **To configure the RTP Port Range and Payload Type:**

■ **Using the Web:**

1. Access the 'Media Streaming' page (**Configuration** tab > **Voice Over IP** menu > **Media Streaming**).

Figure 19-1: Media Streaming Web Fields

2. Configure the RTP Port Range and Payload Type parameters according to the table below, and then click **Submit**.

■ **Using the Configuration file:**

Table 19-2: RTP Port Range and Payload Type Parameters

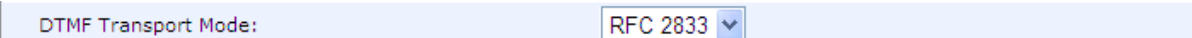| Parameter	Description
DTMF Relay RFC 2833 Payload Type **[voip/media/dtmf_payload]**	Defines the RTP payload type used for RFC 2833 DTMF relay packets. The valid range is 96 to 127. The default value is 101.
RTP Port Range **[voip/media/media_port]**	Defines the starting port range for Real Time Protocol (RTP) voice transport. The valid range is 1024 to 65535. The default value is 4000.

19.3   Configuring RTP QoS
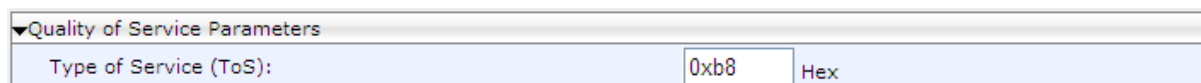
RTP QoS can be configured using the Web or Configuration File, as described below.

➢ **To configure RTP QoS:**

■ **Using the Web:**

1. Access the 'Media Streaming' page (**Configuration** tab > **Voice Over IP** menu > **Media Streaming**).

Figure 19-2: QoS Web Fields

2. Configure the RTP QoS parameters according to the table below, and then click **Submit**.

■ **Using the Configuration file:**

Table 19-3: RTP QoS Parameters

Parameter	Description
Type of Service (ToS) **[voip/media/media_tos]**	QoS in hexadecimal format. This is a part of the IP header that defines the type of routing service to tag outgoing voice packets originated from the phone. It informs routers that this packet must receive a specific QoS. The default value is **0xb8**. Values can be set in decimal (e.g. 184) or hexadecimal (e.g. 0xb8).

19.4 Configuring Codecs

Codecs can be configured using the Web or Configuration File, as described below.

➢ **To define the Codecs:**

■ **Using the Web:**

1. Access the 'Media Streaming' page (**Configuration** tab > **Voice Over IP** menu > **Media Streaming**).

Figure 19-3: Codecs Web Fields

Codec Priority	Codec Type	Packetization Time (milliseconds)
1st Codec	G.722	20
2nd Codec	G.711, 64 Kbps, u-Law	20
3rd Codec	G.711, 64 Kbps, A-Law	20
4th Codec	G.729, 8 Kbps	20
5th Codec	None	10

2. Configure the Codecs parameters according to the table below, and then click **Submit**.

■   **Using the Configuration File:**

Table 19-4: Codec Parameters

Parameter	Description
voip/codec/codec_info/%d/enabled	Determines the codecs that you want to implement and their priority. Up to five codecs can be configured, where the first codec (i.e., **voip/codec/0/…**) has the highest priority. To make a call, at least one codec must be configured. In addition, for best performance it is recommended to select as many codecs as possible. When you start a call to a remote party, your available codecs are compared with the remote party's to determine the codec to use. If there is no codec that both parties have made available, the call attempt fails. Note that if more than one codec is common to both parties, you cannot force which of the common codecs are used by the remote party's client. If you do wish to force the use of a specific codec, configure the list with only that specific codec. The *%d* variable stands for the priority: ▪ **[0]** - Disabled ▪ **[1]** (default) - Enabled
Codec Type **[voip/codec/codec_info /%d/name]**	Name of the codec. The variable *%d* depicts the index number of the codec entry and its priority, where the first codec (i.e. **voip/codec/codec_info/0/name=…**) has the highest priority. The valid codec parameters are: ▪ **[G722]** G.722 ▪ **[PCMA]** G.711 A-Law ▪ **[PCMU]** G.711 Mu-Law ▪ **[G729]** G.729 ▪ **[G723]** G.723 ▪ **[RTA]** (Narrowband Microsoft RT Audio) ▪ **[RTA_WB]** (Wideband Microsoft RT Audio) For example, **voip/codec/codec_info/0/name=G722**. **Note**: Specific codecs require specific firmware files. For more information, refer to the Release Notes.
Packetization Time **[voip/codec/codec_info /%d/ptime]**	Packetization time - length of the digital voice segment that each packet holds. The default is 20 millisecond packets, excluding G.723 which is 30 millisecond packets.
G.723 Bitrate **[voip/codec/g723_bitrate]**	Low or high bit rate for G.723. ▪ **[LOW]** Low ▪ **[HIGH]** High (default)
[voip/codec/g722_bitrate]	G.722 bit rate. ▪ **[G722_64K]** (default) ▪ **[G722_56K]** ▪ **[G722_48K]** **Note:** Currently, only 64bps is supported.
/system/activation_keys/amr_coder	Activation key (string) required to unlock AMR coder (relevant for supporting firmware only).

Reader's Notes

20   Voice Settings

The procedures for configuring voice settings are described below.

20.1   Configuring Jitter Buffer

Jitter Buffer can be configured using the Web or Configuration File, as described below.

➢ **To define Jitter Buffer parameters:**

1. Access the 'Voice' page (**Configuration** tab > **Voice Over IP** menu > **Voice**).

Figure 20-1: Voice Web Fields

2. Configure the Jitter Buffer parameters according to the table below, and then click **Submit**.

■ **Using the Configuration File:**

Table 20-1: Jitter Buffer Parameters

Parameter	Description
Minimum Delay **[voip/audio/jitter_buffer/min _delay]**	The initial and minimal delay of the adaptive jitter buffer mechanism, which compensates for network problems. The value should be set according to the expected average jitter in the network (in milliseconds). The valid range is 10 to 150. The default value is 35.
Optimization Factor **[voip/audio/jitter_buffer/opti mization_factor]**	The adaptation rate of the jitter buffer mechanism. Higher values cause the jitter buffer to respond faster to increased network jitter. The valid range is 0 to 13. The default value is 7.

20.2   Configuring Silence Compression
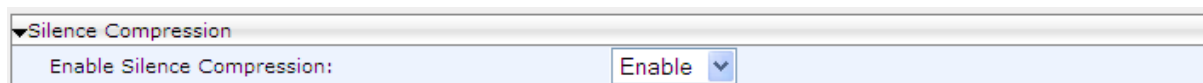
Silence Compression can be configured using the Web or Configuration File, as described below.

➢ **To define the Silence Compression parameters:**

■ **Using the Web:**

1.   Access the 'Voice' page (**Configuration** tab > **Voice Over IP** menu > **Voice**).

Figure 20-2: Silence Compression Web Fields

2.   Configure Silence Compression parameters according to the table below, and then click **Submit**.

■ **Using the Configuration File:**

Table 20-2: Silence Compression Parameters

Parameter	Description
Enable Silence Compression **[voip/audio/silence_compression/enabled]**	Enables silence compression for reducing network bandwidth consumption. ▪ **[0]** Disable (default) ▪ **[1]** Enable

20.3   Configuring Echo Cancellation

Echo Cancellation can be configured using the Configuration File, as described below.

Table 20-3: Echo Cancellation Parameter

Parameter	Description
voip/audio/echo_cancellation/enabled	Enables echo cancellation. ▪ **[0]** - Disable ▪ **[1]** (default) – Enable **Note:** Disabling echo cancellation should be done for testing purposes only.

Reader's Notes

21   Lines/SIP Accounts Settings

This section shows how to configure lines.

21.1   Configuring Lines/SIP Accounts using Phone Interface

Lines/SIP Accounts can be configured on the 310HD, 320HD and 420HD IP Phones as shown below.

21.1.1   310HD IP Phone

The SIP Accounts submenu allows you to configure parameters related to the 310HD IP Phone's SIP account.

➢ **To configure the Lines/SIP Accounts using phone interface:**

1. Access the SIP Accounts screen (**MENU** key > **Administration** menu > **SIP Accounts**).
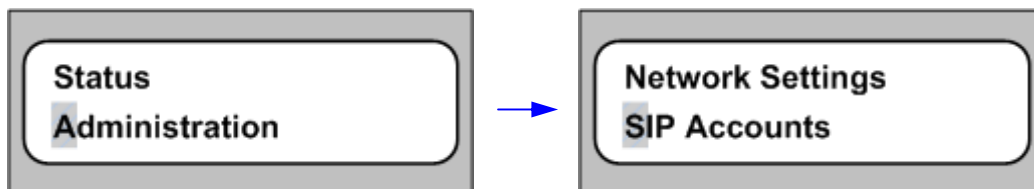
The following screen appears:
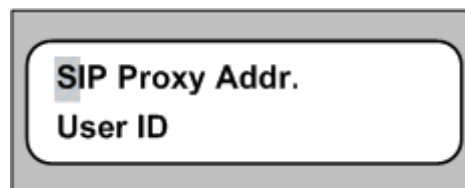
2. Define the SIP proxy IP address.

3. Select the **SIP Proxy Addr.** option (using the ▲ and ▼ Navigation keys), and then press the ENTER key; the following screen appears:
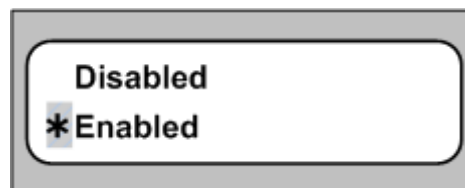
4. Select one of the following options (using the ▲ and ▼ Navigation keys), and then press the ENTER key (an asterisk appears alongside the selected option):

- **Disabled:** Disables the SIP proxy
- **Enabled:** Enables the SIP proxy

5. Press the **ENTER** key again; you are prompted to enter the IP address of the proxy server:

```
ProxyServer
10.16.2.56
```
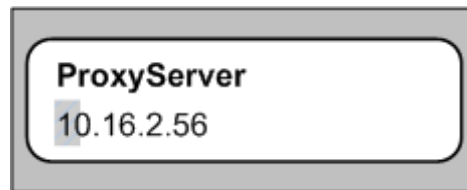
6. Enter the **IP address**, and then press the **ENTER** key; you are returned to the SIP Accounts options.

7. Define the remaining SIP proxy parameters, by selecting (using the ▲ and ▼ Navigation keys) the required parameter:

- **User ID**
- **Display Name:** Caller ID
- **Auth. Name:** Authentication name
- **Auth. Password:** Authentication password

For each parameter, once you have entered the required value, press the ENTER key.

8. Select the **Save** option (using the ▲ and ▼ Navigation keys), and then press the ENTER key; your SIP account settings are saved.

21.1.2   320HD IP Phone

You need to configure parameters related to the phone's SIP account. This also allows you to set up the phone with up to four lines, each with its own extension phone number. These lines correspond to the LINE keys on your phone. For each line you need to configure a SIP account.

➢ **To configure Lines/SIP Accounts using the phone interface:**

1. Access the SIP Accounts screen (**MENU** key > **Administration** menu > **SIP Accounts** submenu).

```
 Menu                    04:00        Administration           02:35
  3. Speed Dial              ▲          1. Network Settings
  4. Settings                           2. SIP Accounts
  5. Status                             3. Restore Defaults
  6. Administration                     4. Restart
 Select              Back             Select              Back
```

The following screen appears:

```
 SIP Accounts            00:04

  1. Line 202
  2. Line 204


 Select   Add    Delete   Back
```

2. To add a new line extension (SIP account), press the **Add** softkey (otherwise, to define an existing SIP account, skip to Step 3); the following screen appears:

```
 SIP Accounts            00:06

  1. Line 202
  2. Line 204
  3. Line 2

 Select   Add    Delete   Back
```

Added Line Extension
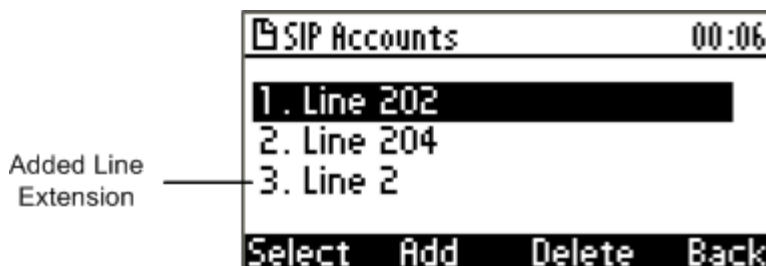
3. Choose (using the ▲ and ▼ Navigation keys) the line, and then press the **Select** softkey; the SIP Details screen appears:
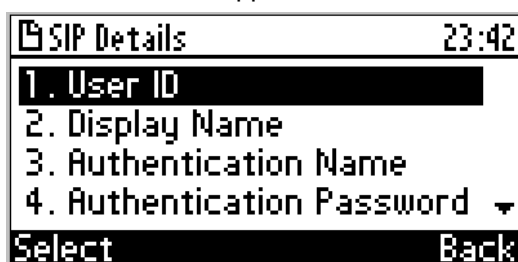
```
 SIP Details             23:42
  1. User ID
  2. Display Name
  3. Authentication Name
  4. Authentication Password  ▼
 Select                  Back
```

4. Choose the required SIP parameter, and then press the **Select** softkey to define it:
   - "User ID"
   - "Display Name"
   - "Authentication Name"
   - "Authentication Password"
   - "SIP Proxy Address" - SIP proxy server's address
5. After each parameter setting, press the **Save** softkey to save the setting.
6. When you have completed all the SIP account settings, press the **Back** softkey until you are prompted that the phone is about to reboot itself. The phone reboots automatically and the warning message 'Phone is rebooting to apply new settings' is indicated.

21.1.3 420HD IP Phone

Configuration of Lines/SIP Accounts on the 420HD IP phone is identical to that on the 320HD IP phone.

➢ **To configure Lines/SIP Accounts using the phone interface:**

1. Access the SIP Accounts screen (**MENU** key > **Administration** menu > **SIP Accounts** submenu).
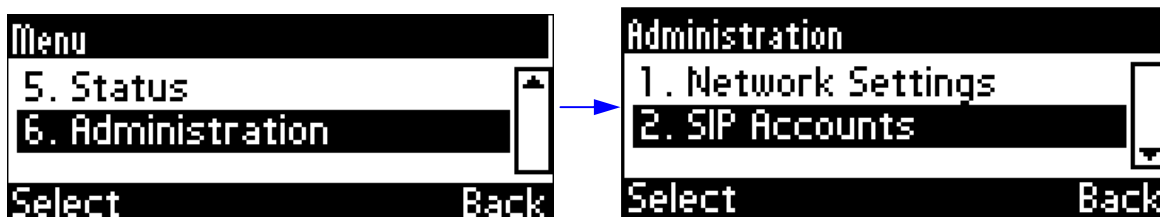
The following screen appears:

2. To add a new line extension (SIP account), press the **Add** softkey (or skip to Step 3 to define an existing SIP account).

3. Press the navigation control's lower rim to navigate to the added line, and then press the **Select** softkey; the SIP Details screen appears.

```
SIP Details
1. User ID
2. Display Name
Select                      Back
```

4. Choose the required SIP parameter, and then press the **Select** softkey to define it:

- "User ID"
- "Display Name"
- "Authentication Name"
- "Authentication Password"
- "SIP Proxy Address" - SIP proxy server's address

5. After each parameter setting, press the **Save** softkey to save the setting.

6. When you have completed all the SIP account settings, press the **Back** softkey until you are prompted that the phone is about to reboot itself. The phone reboots automatically and a warning message 'Phone is rebooting to apply new settings' is indicated.

```
Phone is rebooting
to apply new settings...
```

21.2   Configuring Lines using Web and Configuration File
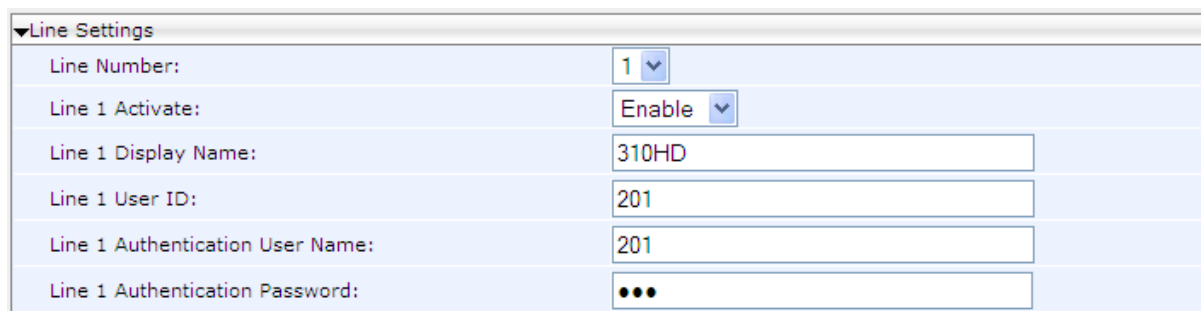
Before you can make a call on your phone, you must configure a phone line. Lines can be configured using the Web or Configuration File, as described below.

➢ **To configure lines:**

■ **Using the Web:**

    1.   Access the 'Line Settings' page (**Configuration** tab > **Voice Over IP** menu > **Line Settings**).

Figure 21-1: Voice Web Fields

    2.   Configure the Line settings according to the parameters in the table below, and then click **Submit**.

■ **Using the Configuration File:**

Table 21-11: Line Parameters

Parameter	Description
Note: The value *%d* refers to the line number.	
Line Activate **[voip/line/%d/enabled]**	Enables the line. ▪ **[0]** Disable ▪ **[1]** Enable The default for Line-0 is 1 (enabled); for the other lines it is 0 (disabled).
Line User ID **[voip/line/%d/id]**	Lines VoIP user's ID for identification to initiate and accept calls. The user's ID can be up to 30 characters.
Line Display Name **[voip/line/%d/description]**	Arbitrary name to intuitively identify the line and that is displayed to remote parties as your caller ID.
Line Authentication User Name **voip/line/%d/auth_name**	User name provided to you from the VoIP service provider. This is used when sending a response to Unauthorized or Proxy Authentication Requested (401/407). The authentication name can be up to 35 characters.
Line Authentication Password **voip/line/%d/auth_password**	Password provided to you from the VoIP Service Provider. This is used when sending a response to Unauthorized or Proxy Authentication Requested (401/407). The authentication password can be up to 35 characters.

Parameter	Description
/voip/line/%d/extension_display	Set the string that is displayed for local extension. If not set, the local extension display will be the user ID (self-number).

Note: You can activate DnD per phone line. See Section 22.7 on page 142.

Reader's Notes

22   Supplementary Services

You can configure various supplementary services supported by your phone such as Call Waiting, Call Forwarding, Three-way Conferencing, and Message Waiting Indication (MWI).

22.1   Selecting the Application Server

By default, the phone is set for a generic application server. However, you can select a specific third-party application server as described below. See Appendix A on page 267 for more information.

> **Note:**   Configuration of specific supplementary services depends on the third-party application server used in your organization.

Selecting the Application Server can be done by using the Web or Configuration File, as described below.

➢ **To select the application server:**

■ **Using the Web:**

1.   Access the 'Services' page (**Configuration** tab > **Voice Over IP** menu > **Services**).

Figure 20-1: Services Page

2.   Select the desired application server according to the table below, and then click **Submit**.

■ **Using the Configuration file:**

Table 20-1: General Supplementary Services Parameters

Parameter	Description
Type **[voip/services/application_server_type]**	Defines the type of the Application server to which the device is registered. ▪ **[Generic]** Generic (default) ▪ **[Asterisk]** Asterisk ▪ **[BSFT]** BroadSoft ▪ **[Coral]** Coral ▪ **[Metaswitch]** Metaswitch ▪ **[FreeSWITCH]** FreeSWITCH **Note:** In addition to the general supplementary services parameters, parameters (if any) unique to the selected Application server become applicable.

Parameter	Description
/system/current_user_presence_status/enabled	Enables the "presence" feature. DND SK will be replaced by "status"; phone will be show and publish the presence state.

22.2   Configuring Call Waiting
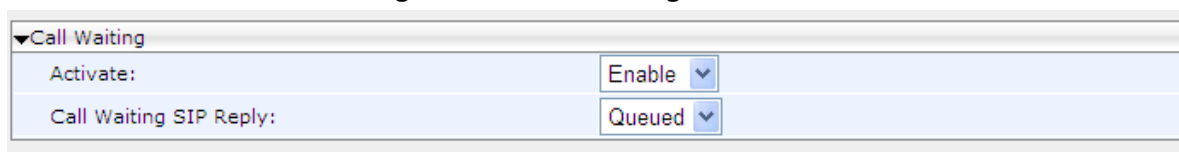
Call Waiting can be configured using the Web or Configuration File, as described below.

➢ **To configure call waiting:**

■ **Using the Web:**

1. Access the 'Services' page (**Configuration** tab > **Voice Over IP** menu > **Services**).

Figure 22-1: Call Waiting Web Fields

2. Configure the Call Waiting parameters according to the table below, and then click **Submit**.

■ **Using the Configuration file:**

Table 22-1: Call Waiting Parameters

Parameter	Description
Activate **[voip/services/call_waiting/enabled]**	Enables the Call Waiting feature. ▪ **[0]** Disable ▪ **[1]** Enable (default)
Call Waiting SIP Reply **[voip/services/call_waiting/sip_reply]**	Determines the SIP response that is sent when another call arrives while a call is in progress: ▪ **[RINGING] Ringing** - 180 Ringing ▪ **[QUEUED] Queued** (default) - 182 Queued

22.3   Configuring Call Forwarding

Call Forwarding can be configured using the Web or Configuration File, as described below.

➢ **To configure call forwarding:**

■ **Using the Web:**

   1. Access the 'Services' page (**Configuration** tab > **Voice Over IP** menu > **Services**).

Figure 22-2: Call Forwarding Web Fields

   2. Configure the Call Forwarding parameters according to the table below, and then click **Submit**.

■ **Using the Configuration file:**

Table 22-2: Call Forward Parameters

Parameter	Description
voip/line/%d/call_forward/enabled	Enables the Call Forward feature. ▪ **[0]** Disable ▪ **[1]** Enable (default)
Call Forward Type **[voip/line/%d/call_forward/type]**	Determines the condition upon which incoming calls are forwarded to another destination: ▪ **[Unconditional]** Unconditional - incoming calls are forwarded independently of the status of the line. ▪ **[Busy]** Busy - incoming calls are forwarded only if the phone is busy. ▪ **[No_Reply]** No Reply (default) - incoming calls are forwarded only if the phone does not answer before a user-defined timeout.
Forward on No Reply Timeout **[voip/line/%d/call_forward/timeout]**	If calls are forwarded when the condition is No-Reply, then this parameter defines the time (in seconds) after which incoming calls are forwarded when this is no reply. The valid range is 0 to 7200. The default value is 6.
Forward Destination **[voip/line/%d/call_forward/destination]**	The destination to which the call is directed when call forward is activated.

Parameter	Description
Activate **[voip/line/%d/call_forward/active]**	Activates call forwarding, if it has been enabled (using the parameter **voip/line/%d/call_forward/enabled**). ▪ **[0]** (default) - Disable ▪ **[1]** Enable **Note:** Call forwarding can also be activated using the LCD screen (common).

22.4   Configuring Three-way Conferencing
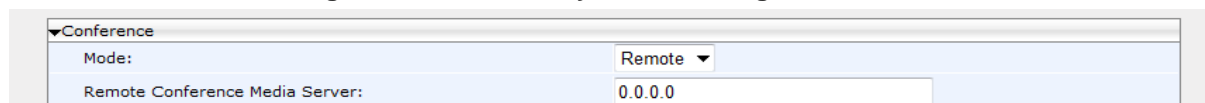
Three-way conferencing can be configured using the Web or Configuration File, as described below.

➢ **To configure three-way conferencing:**

■ **Using the Web:**

1. Access the 'Services' page (**Configuration** tab > **Voice Over IP** menu > **Services**).

Figure 22-3: Three-way Conferencing Web Fields

▼Conference	
Mode:	Remote ▼
Remote Conference Media Server:	0.0.0.0

2. Configure the Three-way conferencing parameters according to the table below, and then click **Submit**.

■ **Using the Configuration file:**

Table 22-3: Three-way Conferencing Parameters

Parameter	Description
Mode **[/voip/services/conference/mode]**	Sets the conference mode (when establishing 3-Way Conference). **[LOCAL]** = phone will establish the conference by itself. **[REMOTE]** = phone will use remote media server for establishing the conference.
Remote Conference Media Server **[/voip/services/conference/conf_ms_addr]**	Media server for establishing remote conference. Relevant only in case the conference mode is REMOTE.

22.5 Configuring Automatic Dialing
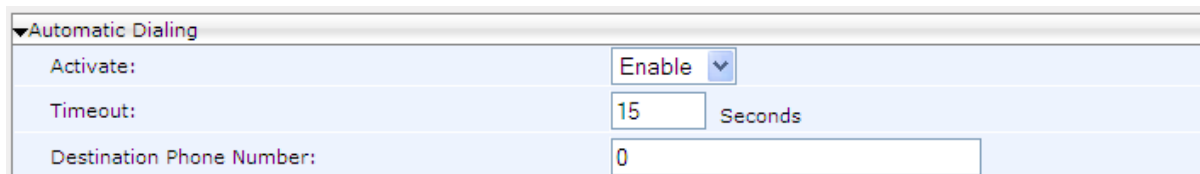
Automatic Dialing can be configured using the Web or Configuration File, as described below.

➢ **To define the Automatic Dialing parameters:**

■ **Using the Web:**

1. Access the 'Dialing' page (**Configuration** tab > **Voice Over IP** menu > **Dialing**).

Figure 22-4: Automatic Dialing Web Fields

2. Configure dialing options according to the parameters in the table below, and then click **Submit**.

■ **Using the Configuration File:**

Table 22-4: Automatic Dialing Parameters

Parameter	Description
Activate **[voip/dialing/auto_dialing/enabled]**	Determines whether automatic dialing is enabled (i.e., phone number is automatically dialed when you off-hook the phone). ▪ **[0]** Disable (default) ▪ **[1]** Enable
Timeout **[voip/dialing/auto_dialing/timeout]**	Timeout (in seconds) before automatic dialing occurs after the phone is off-hooked. When set to 0, automatic dialing is performed immediately. The valid range is 0 to 120. The default value is 15.
Destination Phone Number **[voip/dialing/auto_dialing/destination]**	The number that is automatically dialed when the phone is off-hooked. The valid value can be up to 32 characters.

22.6 Configuring Automatic Answer

The Automatic Answer feature is configured using the Configuration File parameters described in the table below.

Table 22-5: Automatic Answer Parameters

Parameter	Description

voip/auto_answer/enabled	Enables the Automatic Answering feature.
	▪ **[0]** Disable (default)
	▪ **[1]** Enable
	When this parameter is enabled and an incoming SIP INVITE message is received containing information that informs the IP phone to automatically answer the call, the phone answers the call immediately or after a timeout, depending on the auto-answer type specified in the INVITE message:
	▪ **Phone answers after a timeout:** The phone automatically answers the call after a timeout if the INVITE message includes a SIP Call-Info header with a tag value, "answer-after=" set to a number representing the timeout. During the timeout interval, the phone rings normally. If the call is answered or rejected during this interval, then the automatic answering mechanism is not used. However, if the phone is left to ring throughout the timeout interval, it automatically answers the call once this timeout expires.
	▪ **Phone answers immediately:** The phone answers the call immediately in any of the following cases:
	  ▪ If the SIP Alert-Info header contains the tag value, "ring answer".
	  ▪ If the SIP Alert-Info header contains the tag value, "info=alert-autoanswer".
	Notes:
	▪ If the SIP Call-Info header includes all the above answer types or any two different types (i.e., "answer-after=", "ring answer", and "alert-autoanswer"), the answer-after= type takes precedence.
	▪ If there is an existing call when an INVITE message for automatic answer is received, the existing call is automatically put on hold.

voip/talk_event/enabled	Enables the "talk" event feature. ▪ **[0]** Disable (default) ▪ **[1]** Enable The phone automatically answers an incoming call if it receives a SIP NOTIFY message with the "talk" event. If a call is already in progress, the call is put on hold and the incoming call is answered.

22.7 Configuring Do Not Disturb

Do not Disturb (DnD) can be configured using the Web or Configuration File, as described below.

> **Note:** For the 320HD IP Phone, DnD can be activated per phone line.

➢ **To configure DnD:**

■ **Using the Web:**

1. Access the 'Services' page (**Configuration** tab > **Voice Over IP** menu > **Services**).

Figure 22-5: DnD Web Fields

2. Select the desired application server according to the table below, and then click **Submit**.

■ **Using the Configuration file:**

Table 22-6: Do Not Disturb (Services) Parameters

Parameter	Description
Activate **[voip/services/do_not_disturb/enabled]**	Enables the DnD feature. ▪ **[0]** Disable ▪ **[1]** Enable (default)
Line Number	Defines the extension line for which you want to activate DnD
voip/line/%d/do_not_disturb/activated	Activates the DnD feature per phone line, if DnD is enabled using the parameter **voip/services/do_not_disturb/enabled**. ▪ **[0]** - Activate (default) ▪ **[1]** - Deactivate **Note:** DnD can also be activated using the LCD screen interface (more common).

22.8   Configuring Call Pickup

Since the Call Pickup feature is relevant only when Busy Lamp Field (BLF) is activated, the call pickup parameters appear as BLF related parameters.

➢ **To configure Call Pickup :**

■ **Using the Web:**

1.   Access the 'Services' page (**Configuration** tab > **Voice Over IP** menu > **Services**).

Figure 22-6: Call Pick Up Web Fields

BLF Support	
Activate:	Enable ▾
Call Pick Up:	Enable ▾
BLF Subscription Period:	3600 Seconds

2.   Under the **BLF Support** group, ensure that the 'Activate' field is set to "Enable".
3.   Configure Call Pickup according to the parameters in the table below, and then click **Submit**.

Table 22-7: Call Pickup Parameters

Parameter	Description
Call Pick Up **[/voip/services/call_pickup/enabled]**	Allows call pickup by pressing on the relevant BLF key when the state of the remote phone is "ringing". ▪ **[0] Disable** ▪ **[1] Enable**
[voip/services/call_pickup/access_code]	The phone supports the Call Pick-Up feature, whereby the user can answer someone else's telephone call by pressing a user-defined sequence of phone keys. When the user dials the user-defined digits plus the other phone number, the incoming call from the other phone is forwarded to the user's phone. The default key sequence is **∗∗**. For example, to pick up a call for extension 5000 dial **∗∗5000**.

22.9 Configuring Message Waiting Indication
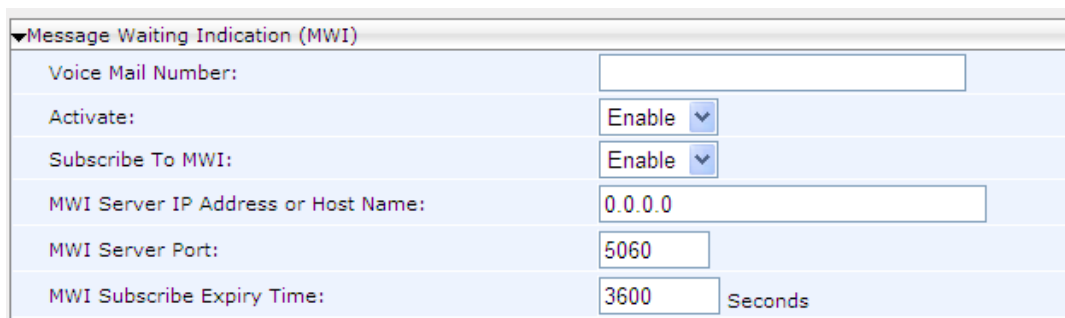
Message Waiting Indication (MWI) can be configured using the Web or Configuration File, as described below.

➢ **To configure MWI:**

■ **Using the Web:**

1. Access the 'Services' page (**Configuration** tab > **Voice Over IP** menu > **Services**).

Figure 22-7: MWI Web Fields

2. Configure the MWI parameters according to the table below, and then click **Submit**.

■ **Using the Configuration file:**

Table 22-8: Message Waiting Indication Parameters

Parameter	Description
Activate **[voip/services/msg_waiting_ind/enabled]**	Enables the MWI feature. ▪ **[0]** Disable ▪ **[1]** Enable (default)
Subscribe To MWI **[voip/services/msg_waiting_ind/subscribe]**	Determines whether the phone registers to an MWI server. ▪ **[0]** Disable (default) ▪ **[1]** Enable
MWI Server Port **[voip/services/msg_waiting_ind/subscribe_port]**	The port number of the MWI server. The valid range is 1024 to 65535. The default value is 5060.
MWI Server IP Address or Host Name **[voip/services/msg_waiting_ind/subscribe_address]**	The IP address or host name of the MWI server. The default value is 0.0.0.0.
MWI Subscribe Expiry Time **[voip/services/msg_waiting_ind/expiraition_timeout]**	The interval between the MWI Subscribe messages. The valid range is 0 to 86400. The default value is 3600.
Voice Mail Number **[voip/services/msg_waiting_ind/voice_mail_number]**	Defines the extension number for accessing your voice mail messages. The valid value is up to 64 characters.

Parameter	Description
voip/services/msg_waiting_ind/always_send_port	If the SIP port is the default port (i.e. 5060), then remove it from the Request-URI of the MWI SUBSCRIBE. ▪ **[0]** Disable ▪ **[1]** Enable (default)

22.10 Configuring Busy Lamp Field

Busy Lamp Field (BLF) can be configured using the Web or Configuration File, as described below.
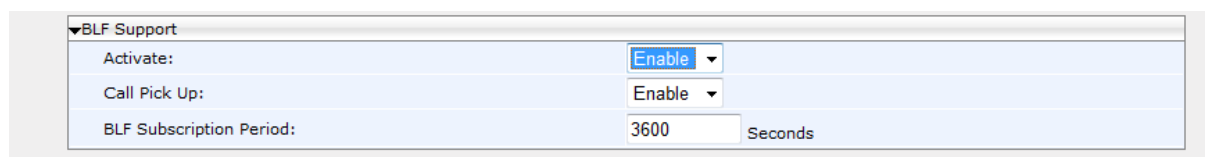
> **Note:** BLF is only applicable to the **320HD IP Phone**.

➢ **To configure BLF:**

■ **Using the Web:**

1. Access the 'Services' page (**Configuration** tab > **Voice Over IP** menu > **Services**).

Figure 22-8: BLF Support Web Fields

▼BLF Support	
Activate:	Enable ▼
Call Pick Up:	Enable ▼
BLF Subscription Period:	3600 Seconds

2. Configure the BLF parameters according to the table below, and then click **Submit**.

■ **Using the Configuration file:**

Table 22-9: BLF Parameters

Parameter	Description
Activate **[voip/services/busy_lamp_field/enabled]**	Enables the BLF feature: ▪ **[0]** Disable ▪ **[1]** Enable (default)
BLF Subscription Period **[voip/services/busy_lamp_field/subscription_period]**	The interval between BLF and SIP SUBSCRIBE messages. The valid range is 0 to 86400. The default value is 3600.
User Resource List **[voip/services/busy_lamp_field/uri]**	The user resource list. This must be the username (not the domain name). For example, if the URI resource list is **mylist@server.com**, then only the value **mylist** must be entered. The valid value is up to 64 characters. **Note:** This parameter is applicable only if the parameter **voip/services/application_server_type** is set to **BSFT**.

Parameter	Description
Use Registrar as Application Server Address **[voip/services/busy_lamp_field/application_server/use_registrar]**	Determines whether to use the registrar as the application server address. When enabled, there is no need to configure the application server address or domain name separately. ▪ **[0]** Disable (default) ▪ **[1]** Enable **Note:** This parameter is applicable only if the parameter **voip/services/application_server_type** is set to **BSFT**.
Use Registrar as Application Server Address **[voip/services/busy_lamp_field/application_server/addr]**	The IP address or host name of the application server. The valid value is up to 64 characters. The default value is 0.0.0.0. **Note:** This parameter is applicable only if the parameter **voip/services/application_server_type** is set to **BSFT** and **voip/services/busy_lamp_field/application_server/use_registrar** is set to 0.

22.11 Configuring Advice of Charge
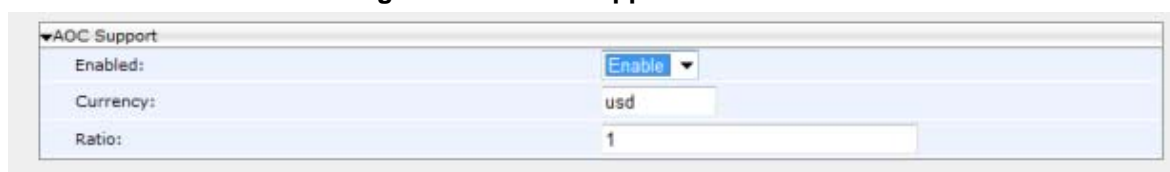
Advice of Charge (AOC) can be configured using the Web or Configuration File, as described below.

➢ **To configure AOC:**

■ **Using the Web:**

    1. Access the 'Services' page (**Configuration** tab > **Voice Over IP** menu > **Services**).

Figure 22-9: AOC Support Web Fields

    2. Configure the AOC parameters according to the table below, and then click **Submit**.

■ **Using the Configuration File:**

Table 22-10: AOC Parameters

Parameter	Description
Enable **[system/aoc/enabled]**	Enables the "advice of charge" feature. ▪ **[0] Disable** ▪ **[1] Enable**
Currency **[system/aoc/currency]**	Sets the desired currency for AOC display. The string represents the currency name. (e.g., USD , EUR , NIS , etc..)
Ratio **[system/aoc/ratio]**	Sets the conversion ratio from the local currency. The string represents the ratio between the base currency to the set currency with a decimal point),(e.g., : 3.8, 4.95 , 1).

22.12 Enabling Electronic Hook Switch

Electronic Hook Switch (EHS) can be enabled using the Web or Configuration File, as described below.

➢ **To enable EHS:**

■ **Using the Web:**

    1. Access the 'Services' page (**Configuration** tab > **Voice Over IP** menu > **Services**).

Figure 22-10: EHS Web Fields

Electronic Hook Switch: Disable ▾

    2. Configure the EHS parameters according to the table below, and then click **Submit**.

■ **Using the Configuration file:**

Table 22-11: EHS Parameters

Parameter	Description
Electronic Hook Switch **[voip/services/electronic_hook_switch/enabled]**	Enables the EHS DHSG feature. ▪ **[0]** Disable (default) ▪ **[1]** Enable DHSG is the protocol that uses the special AUX port. Supporting headsets can be connected to the AUX port (in addition to the regular headset port). This allows the user to connect and disconnect calls by pressing the button on the headset.

Reader's Notes

23   Volume Levels

The procedures for configuring volume levels are described below.

23.1   Configuring Automatic Gain Control

Automatic Gain Control can be configured using the Web or Configuration File, as described below.

➢ **To configure the Automatic Gain Control:**

■ **Using the Web:**

   1. Access the 'Voice' page (**Configuration** tab > **Voice Over IP** menu > **Voice**).

Figure 23-1: Auto Gain Control Web Fields

   2. Configure the settings according to the parameters in the table below, and then click **Submit**.

■ **Using the Configuration File:**

Table 23-1: Automatic Gain Control Parameters

Parameter	Description
Enable Automatic Gain Control **[voip/audio/gain/automatic_gain_control/enabled]**	Enables the AGC. AGC automatically adjusts the phone's voice volume to compensate for weak or loud signals. ▪ **[0]** Disable (default) ▪ **[1]** Enable
Automatic Gain Control Direction **[voip/audio/gain/automatic_gain_control/direction]**	Determines whether AGC is located before the encoder input (CTL_LOCAL) or after the decoder output (CTL_REMOTE). ▪ **[CTL_REMOTE]** For Remote User (default) - AGC is located after the Decoder output ▪ **[CTL_LOCAL]** For Local User **-** AGC is located before the Encoder input
Target Energy **[voip/audio/gain/automatic_gain_control/target_energy]**	The required output energy (in dBm) of the AGC. The valid range is -31 to 0 (dB). The default value is -19.

23.2   Configuring Tone Volume

Tone volume can be configured using the Web or Configuration File, as described below.

➢ **To configure tone volume:**

■ **Using the Web:**

1. Access the 'Volume Setting' page (**Configuration** tab > **Voice Over IP** menu > **Volume Settings**).

Figure 23-2: Tone Volume Web Field

| Tone Volume: | -10dB |

2. Configure the tones volume settings according to the parameters in the table below, and then click **Submit**.

■ **Using the Configuration file:**

Table 23-2: Tone Volume Parameter

Parameter	Description
Tone Volume **[voip/audio/gain/tone_signal_level]**	Call progress tone volume. This volume can be modified on-the-fly by pressing the phone's VOLUME key in certain scenarios. The valid range is 1 to 31 (-dB). The default value is 10 (-10dB).

23.3   Configuring Ringer Volume

The ringer volume can be configured using the Web or Configuration File, as described below.

➢   **To configure the ringer volume:**

■   **Using the Web:**

1.   Access the 'Volume Setting page (**Configuration** tab > **Voice Over IP** menu > **Volume Settings**).

Figure 23-3: Ringer Volume Web Field

Ringer Volume:	0dB ▼

2.   Configure the ringer volume settings according to the parameters in the table below, and then click **Submit**.

■   **Using the Configuration file:**

Table 23-3: Ringer Volume Parameters

Parameter	Description
Ringer Volume **voip/audio/gain/ringer_signal_level**	Ringing tone volume. This volume can be modified on-the-fly by pressing the phone's VOLUME key when the phone is in idle state. The valid range is [-31] to [31] dB

23.4   Configuring Speakerphone (Hands Free) Volume

The speakerphone (Hands Free) volume can be configured using the Web or Configuration File, as described below.

➢ **To configure speakerphone (Hands Free) volume:**

■ **Using the Web:**

1. Access the 'Volume Setting' page (**Configuration** tab > **Voice Over IP** menu > **Volume Settings**).

Figure 23-4: Hands Free Web Fields

Hands Free Digital Output:	3dB
Hands Free Digital Input:	0dB
Hands Free Analog Output:	0dB
Hands Free Analog Input:	39.0dB

2. Configure the Volume settings according to the parameters in the table below, and then click **Submit**.
3. Access the 'Services' page (**Configuration** tab > **Voice Over IP** menu > **Volume Settings**).

Figure 23-5: Additional Speaker Volume Web Field

▼Volume Setting	
Additional Speaker Volume:	3dB

4. Configure the speakerphone volume according to the parameters in the table below, and then click **Submit**.

Table 23-13: Speakerphone (Hands Free) Parameters

Parameter	Description
Hands-free Gain Parameters **Note:** Values are in decibels (dB) and represented as follows: ▪ Negative values: use the word "minus" (e.g. =minus9db). ▪ Positive values: use the word "plus" (e.g. =plus9db). ▪ Decimal places: use underscore instead of period (e.g. plus19_5db).	
Hands Free Digital Output **[voip/audio/gain/handsfree_digital_output_gain]**	Digital output gain (in dB). The valid range is (-32) to 31 (dB), where -32 is mute.
Hands Free Digital Input **[voip/audio/gain/handsfree_digital_input_gain]**	Digital input gain (in dB). The valid range is (-32) to 31 (dB), where -32 is mute.

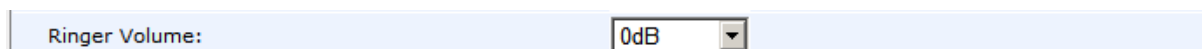| Parameter	Description
Hands Free Analog Output **[voip/audio/gain/handsfree_analog_output_gain]**	Analog output gain (in dB). Valid values: **[0db]**, **[minus1_5db]**, **[minus3db]**, **[minus4_5db]**, **[minus6db]**, **[minus7_5db]**, **[minus9db]**, **[minus10_5db]**, **[minus12db]**, **[minus13_5db]**, **[minus15db]**, **[minus16_5db]**, **[minus18db]**, **[minus19_5db]**, **[minus21db]**, **[minus22_5db]**, **[minus24db]**, **[minus25_5db]**, **[minus27db]**, **[minus28_5db]**, **[minus30db]**, **[minus31_5db]**, **[minus33db]**, **[minus34_5db]**, **[minus36db]**, **[minus37_5db]**, **[minus39db]**, **[minus39db]**, **[minus42db]**, **[minus48db]**, **[minus54db]**, **[MUTE]**
Hands Free Analog Input **[voip/audio/gain/handsfree_analog_input_gain]**	Analog input gain (in dB). Valid values: **[0db]**, **[plus1_5db]**, **[plus3db]**, **[plus4_5db]**, **[plus6db]**, **[plus7_5db]**, **[plus9db]**, **[plus10_5db]**, **[plus12db]**, **[plus13_5db]**, **[plus15db]**, **[plus16_5db]**, **[plus18db]**, **[plus19_5db]**, **[plus21db]**, **[plus22_5db]**, **[plus24db]**, **[plus25_5db]**, **[plus27db]**, **[plus28_5db]**, **[plus30db]**, **[plus31_5db]**, **[plus33db]**, **[plus34_5db]**, **[plus36db]**, **[plus37_5db]**, **[plus39db]**, **[plus40_5db]**, **[plus42db]**, **[plus48db]**, **[plus54db]**, **[MUTE]**
Additional Speaker Gain **[voip/audio/gain/additional_speaker_gain]**	Additional parameter for speaker gain configuration. ▪ **[0]** 0dB ▪ **[1]** 1dB ▪ **[2]** 2dB ▪ **[3]** 3dB

23.5   Configuring Handset Volume

The handset volume can be configured using the Web or Configuration File, as described below.

➢ **To configure handset volume:**

■ **Using the Web:**

1. Access the 'Volume Setting page (**Configuration** tab > **Voice Over IP** menu > **Volume Settings**).

Figure 23-6: Handset Volume Settings Page

Handset Digital Output:	0dB
Handset Digital Input:	0dB
Handset Analog Output:	-9.0dB
Handset Analog Input:	19.5dB
Handset Analog Sidetone Gain:	-12dB

2. Configure the handset volume settings according to the parameters in the table below, and then click **Submit**.

■ **Using the Configuration File:**

Table 23-14: Handset Gain Parameters

Parameter	Description
Handset Gain Parameters **Note:** Values are in decibels (dB) and represented as follows: ▪ Negative values: use the word "minus" (e.g. =minus9db). ▪ Positive values: use the word "plus" (e.g. =plus9db). ▪ Decimal places: use underscore instead of period (e.g. plus19_5db).	
Handset Digital Output **[voip/audio/gain/handset_digital_output_gain]**	Digital output gain (in dB). The valid range is (-32) to 31 (dB), where -32 is mute.
Handset Digital Input **[voip/audio/gain/handset_digital_input_gain]**	Digital input gain (in dB). The valid range is (-32) to 31 (dB), where -32 is mute.

Parameter	Description
Handset Analog Output **[voip/audio/gain/handset_analog_output_gain]**	Analog output gain (in dB). Valid values: **[0db]**, **[minus1_5db]**, **[minus3db]**, **[minus4_5db]**, **[minus6db]**, **[minus7_5db]**, **[minus9db]**, **[minus10_5db]**, **[minus12db]**, **[minus13_5db]**, **[minus15db]**, **[minus16_5db]**, **[minus18db]**, **[minus19_5db]**, **[minus21db]**, **[minus22_5db]**, **[minus24db]**, **[minus25_5db]**, **[minus27db]**, **[minus28_5db]**, **[minus30db]**, **[minus31_5db]**, **[minus33db]**, **[minus34_5db]**, **[minus36db]**, **[minus37_5db]**, **[minus39db]**, **[minus39db]**, **[minus42db]**, **[minus48db]**, **[minus54db]**, **[MUTE]**
Handset Analog Input **[voip/audio/gain/handset_analog_input_gain]**	Analog input gain (in dB). Valid values: **[0db]**, **[plus1_5db]**, **[plus3db]**, **[plus4_5db]**, **[plus6db]**, **[plus7_5db]**, **[plus9db]**, **[plus10_5db]**, **[plus12db]**, **[plus13_5db]**, **[plus15db]**, **[plus16_5db]**, **[plus18db]**, **[plus19_5db]**, **[plus21db]**, **[plus22_5db]**, **[plus24db]**, **[plus25_5db]**, **[plus27db]**, **[plus28_5db]**, **[plus30db]**, **[plus31_5db]**, **[plus33db]**, **[plus34_5db]**, **[plus36db]**, **[plus37_5db]**, **[plus39db]**, **[plus40_5db]**, **[plus42db]**, **[plus48db]**, **[plus54db]**, **[MUTE]**
Handset Analog Sidetone Gain **[voip/audio/gain/handset_analog_sidetone_gain]**	Analog side tone gain (in db). Valid values: **[minus9db]**, **[minus12db]** (default), **[minus15db]**, **[minus18db]**, **[minus21db]**, **[minus24db]**, **[minus27db]**, **[MUTE]**

23.6 Configuring Headset Volume

The headset volume can be configured using the Web or Configuration File, as described below.

➢ **To configure headset volume:**

■ **Using the Web:**

1. Access the 'Volume Setting page (**Configuration** tab > **Voice Over IP** menu > **Volume Settings**).

Figure 23-7: Headset Web Fields

Headset Digital Output:	0dB
Headset Digital Input:	0dB
Headset Analog Output:	-12.0dB
Headset Analog Input:	33.0dB
Headset Analog Sidetone Gain:	-12dB

2. Configure the headset volume settings according to the parameters in the table below, and then click **Submit**.

■ **Using the Configuration File:**

Table 23-4: Headset Gain Parameters

Parameter	Description
Headset Gain Parameters **Note:** Values are in decibels (dB) and represented as follows: ▪ Negative values: use the word "minus" (e.g. =minus9db). ▪ Positive values: use the word "plus" (e.g. =plus9db). ▪ Decimal places: use underscore instead of period (e.g. plus19_5db).	
Headset Digital Output **[voip/audio/gain/headset_digital_output_gain]**	Digital output gain (in dB). The valid range is (-32) to 31 (dB), where -32 is mute.
Headset Digital Input **[voip/audio/gain/headset_digital_input_gain]**	Digital input gain (in dB). The valid range is (-32) to 31 (dB), where -32 is mute.

Parameter	Description
Headset Analog Output **[voip/audio/gain/headset_analog_output_gain]**	Analog output gain (in dB). Valid values: **[0db]**, **[minus1_5db]**, **[minus3db]**, **[minus4_5db]**, **[minus6db]**, **[minus7_5db]**, **[minus9db]**, **[minus10_5db]**, **[minus12db]**, **[minus13_5db]**, **[minus15db]**, **[minus16_5db]**, **[minus18db]**, **[minus19_5db]**, **[minus21db]**, **[minus22_5db]**, **[minus24db]**, **[minus25_5db]**, **[minus27db]**, **[minus28_5db]**, **[minus30db]**, **[minus31_5db]**, **[minus33db]**, **[minus34_5db]**, **[minus36db]**, **[minus37_5db]**, **[minus39db]**, **[minus39db]**, **[minus42db]**, **[minus48db]**, **[minus54db]**, **[MUTE]**
Headset Analog Input **[voip/audio/gain/headset_analog_input_gain]**	Analog input gain (in dB). Valid values: **[0db]**, **[plus1_5db]**, **[plus3db]**, **[plus4_5db]**, **[plus6db]**, **[plus7_5db]**, **[plus9db]**, **[plus10_5db]**, **[plus12db]**, **[plus13_5db]**, **[plus15db]**, **[plus16_5db]**, **[plus18db]**, **[plus19_5db]**, **[plus21db]**, **[plus22_5db]**, **[plus24db]**, **[plus25_5db]**, **[plus27db]**, **[plus28_5db]**, **[plus30db]**, **[plus31_5db]**, **[plus33db]**, **[plus34_5db]**, **[plus36db]**, **[plus37_5db]**, **[plus39db]**, **[plus40_5db]**, **[plus42db]**, **[plus48db]**, **[plus54db]**, **[MUTE]**
Headset Analog Sidetone Gain **[voip/audio/gain/headset_analog_sidetone_gain]**	Analog side tone gain (in db). Valid values: **[minus9db]**, **[minus12db]**, **[minus15db]**, **[minus18db]**, **[minus21db]**, **[minus24db]**, **[minus27db]**, **[MUTE]**

Reader's Notes

Part VI

Advanced Phone Settings

Reader's Notes

24   Locking and Unlocking the IP Phone

If your phone is deployed with AudioCodes solution for Microsoft Lync Server 2010, you can lock your phone to prevent anyone from using it (such as making and receiving calls). Incoming calls can be answered only if you provide the correct unlock password; outgoing calls can only be made if they are configured as emergency calls (by your administrator).

> **Notes:**
>
> - This feature is applicable only when your phone is deployed with AudioCodes solution for Microsoft Lync Server 2010 and is enabled by your system administrator. For more information, refer to the *Administrator's Manual*.
> - To obtain the unlocking password, contact your system administrator.
> - When the phone is locked, the emergency number, defined by your system administrator, can be dialed.

24.1   Locking and Unlocking the 310HD IP Phone

The procedures below describe how to lock and then unlock your 310HD IP phone.

➢ **To lock the 310HD IP Phone:**

◼ Press the star key for a few seconds.

If the phone is locked and you receive an incoming call, you are prompted to enter the unlock password in order to establish the call, as shown below:

Unlock password:

➢ **To unlock the 310HD IP Phone:**

1. Press the star key for a few seconds; you are prompted to enter the unlock password:
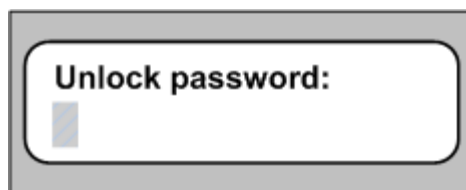
Unlock password:

2. Enter the password, and then press the ENTER key.

24.2 Locking and Unlocking the 320HD IP Phone

The procedures below describe how to lock and then unlock your 320HD IP phone.

24.2.1 Single-Line Mode

The procedures below describe how to lock and then unlock your phone in single-line mode.

➤ **To lock your 320HD IP Phone:**

■ Press the star (*) key for a few seconds (about 3 seconds); the phone locks and the **lock** icon is displayed on the screen, as shown below:

 — Lock Icon

➤ **To unlock your 320HD IP Phone:**

1. Press the star key until you are prompted for the unlock password:

2. Enter the password, and then press the **OK** softkey; the phone is unlocked and the **lock** icon no longer appears on the screen.

24.2.2 Multi-Line Mode

When your phone is configured with multiple lines (extensions), you can perform a lock per extension or for all extensions, as described in the procedure below.

➢ **To lock your 320HD IP Phone:**

1. Press the star key until the Lock screen is displayed:

```
Lock                    01:39AM
All Extensions
Line  569  (Unlocked)
Line  566  (Unlocked)

Lock                    Cancel
```

2. Choose an extension (or **All Extensions** to lock all extensions) that you want to lock, using the ▲ and ▼ Navigation keys, and then press the **Lock** softkey; the extension is locked and the lock icon is displayed with the extension number in the idle screen, as shown below:

Lock Icon ──────

```
569
🔒
───
566
        Sat
         1    01:45
        Jan       am

 📧    Missed  Forward  Status
```

➢ **To unlock your 320HD IP Phone:**

1. Press the star key until the Lock screen is displayed:

```
Lock                    01:50AM
All Extensions
Line  569  (Locked)
Line  566  (Unlocked)

Unlock                  Cancel
```

2. Choose an extension (or **All Extensions** to unlock all extensions) that you want to unlock, using the ▲ and ▼ Navigation keys, and then press the **Unlock** softkey; you are prompted to enter the unlock password, as shown below:

```
                123
Extension 569 is locked.
Please enter password:

|

OK      A/a/1          Cancel
```
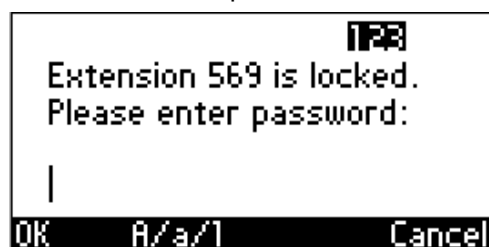
3. Enter the password for unlocking the phone, and then press the **OK** softkey; the extension(s) is unlocked and the **lock** icon no longer appears on the screen.
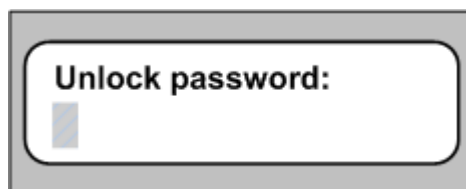
24.3   Locking and Unlocking the 420HD IP Phone

The procedures below describe how to lock and then unlock your 420HD IP phone.

24.3.1   Single-Line Mode

The procedures below describe how to lock and then unlock your phone when it's in single-line mode.

➢ **To lock your 420HD IP Phone:**

■ Press the star (*) key for approximately 3 seconds; the phone locks and the **lock** icon is displayed on the screen:

```
5692 🔒        Thursday          15:29
               18  Oct
      4
Missed  Forward  Status    ☎
```

➢ **To unlock your 420HD IP Phone:**

1. Press the star key until you are prompted for the unlock password:

```
                      123
         Extension .csps2 is locked.
         Please enter password:
         |
OK        A/a/1              Cancel
```
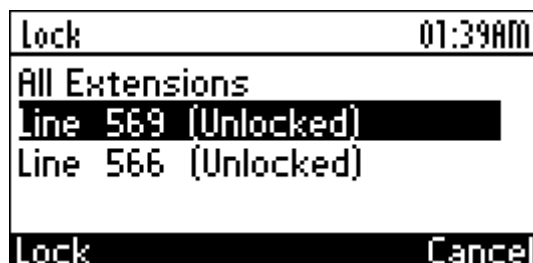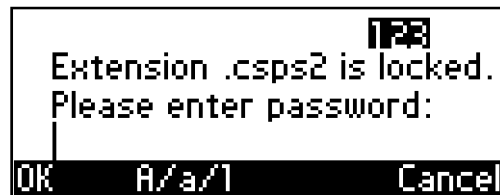
2. Enter the password, and then press the **OK** softkey; the phone is unlocked and the **lock** icon no longer appears on the screen.
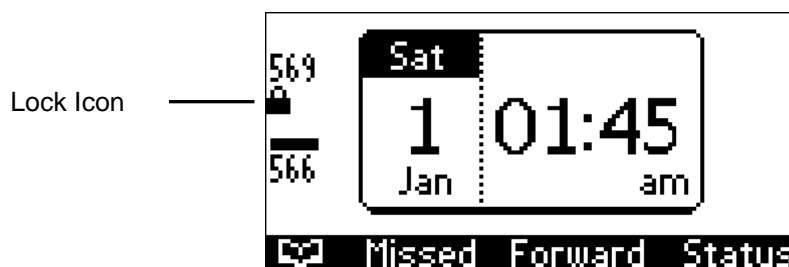
24.3.2   Two-Line Mode

When your phone is configured with two lines (extensions), you can perform a lock per extension or for all extensions, as described in the procedure below.

➢ **To lock your 420HD IP Phone:**

1. Press the star key until the Lock screen is displayed:

```
Lock
All Extensions (Unlocked)
Line lyncsps2 (Unlocked)
Lock                    Cancel
```

2. Press the navigation control's upper or lower rim to navigate to an extension that you want to lock (or **All Extensions** to lock all extensions) and then press the **Lock** softkey; the extension is locked and the lock icon is displayed with the extension number in the idle screen, as shown below:

```
5692 🔒           Thursday        15:35
aaa 📶            18 Oct
Missed  Forward  Status    💬
```

➢ **To unlock your 420HD IP Phone:**

1. Press the star key until the Lock screen is displayed:

```
Lock
All Extensions
Line lyncsps2 (Locked)
Unlock                  Cancel
```

2. Press the navigation control's upper or lower rim to navigate to an extension that you want to unlock (or **All Extensions** to unlock all extensions) and then press the **Unlock** softkey; you are prompted to enter the unlock password, as shown below:

```
                  123
Extension .csps2 is locked.
Please enter password:

OK      A/a/1           Cancel
```
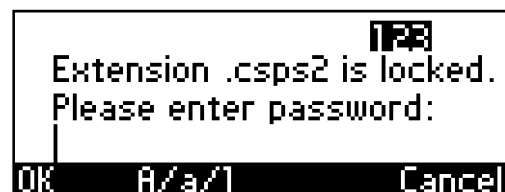
3. Enter the password for unlocking the phone and then press the **OK** softkey; the extension(s) is unlocked and the **lock** icon no longer appears on the screen.

24.4 Using the Configuration File

The phone's Lock / Unlock feature can be configured using the configuration file parameters below:

Table 24-1: Phone Lock/Unlock Parameters

Parameter	Description
/system/lock/[0-0]/enabled	Enables the "phone lock" feature, relevant for supporting servers only.
/system/server_lock_error_code	Refers to specific error code from the server as the "lock" operation trigger. The error code should be 4XX SIP error code.
/system/lock/[0-0]/allow_incoming_calls	Allows incoming calls when the phone is locked. If allowed, the user will need to enter an unlock password to answer an incoming call. If not allowed, the incoming call will be automatically rejected by the phone.
/system/action_url/lock_status	Sets the action URI to get lock status from phone.
/system/action_url/lock	Sets the action URI to lock the phone.
/system/action_url/unlock	Sets the action URI to unlock the phone.

25   Phone Directory

This section describes how to configure the phone directory.

25.1   Corporate Directory

The Corporate Directory can be configured using the Web or Configuration File, as described below.

25.1.1   LDAP-based Corporate Directory

This section describes how to configure Lightweight Directory Access Protocol (LDAP), which is an application protocol for accessing and maintaining distributed directory information services over an IP network. It is fully described under RFC 4510.

➢ **To configure LDAP:**

■ **Using the Web:**

    1. Access the 'LDAP' page (**Configuration** tab > **Advanced Applications** > **LDAP**). If LDAP is set to "Enable", more configuration parameters appear.

Figure 25-1: LDAP Web Fields

    2. Configure the LDAP settings according to the parameters in the table below, and then click **Submit**.

■ **Using the Configuration File:**

Table 25-1: LDAP Parameters

Parameter Name	Description
Active **[system/ldap/enabled]**	Enables or disable LDAP.
Server Address **[system/ldap/server_address]**	Defines the IP address or URL of the LDAP server.

Parameter Name	Description
Port **[system/ldap/port]**	Defines the LDAP service port.
User Name **[system/ldap/user_name]**	Defines the user name used for the LDAP search request.
Password **[system/ldap/password]**	Defines the password of the search requester.
Base **[system/ldap/base]**	Defines the access point on the LDAP tree.
Name Filter **[system/ldap/name_filter]**	Specifies your search pattern for name look ups. For example: When you type in the following field: *(&(telephoneNumber=*)(sn=%)),* the search result includes all LDAP records, which have the 'telephoneNumber' field set and the '("sn"-->surname)' field starting with the entered prefix. When you type in the following field: *(|(cn=%)(sn=%)),* the search result includes all LDAP records which have the ("cn"-->CommonName) OR ("sn"-->Surname) field starting with the entered prefix. When you type in the following field: *(!(cn=%)),* the search result includes all LDAP records which "do not" have the "cn" field starting with the entered prefix.
Name Attribute **[system/ldap/name_attrs]**	Specifies the LDAP name attributes setting, which can be used to specify the "name" attributes of each record which is returned in the LDAP search results. When you type in the following field, for example, *cn sn displayName*", this requires you to specify 'cn-->commonName'. This is the Full name of the user, sn-->Surname, last name or family name and "displayName" fields for each LDAP record.
Number Filter **[system/ldap/number_filter]**	Specifies your search pattern for number look ups. When you type in the following field, for example, *(|(telephoneNumber=%)(Mobile=%)(ipPhone=%))*, the search result is all LDAP records which have the "telephoneNumber" OR "Mobile" OR "ipPhone"field match the number being searched. When you type in the following field: *(&(telephoneNumber=%)(sn=*)),* the search result is all LDAP records which have the "sn" field set and the "telephoneNumber" match the number being searched.

Parameter Name	Description
Number Attribute **[system/ldap/number_attrs]**	Specifies the LDAP number attributes setting, which can be used to specify the "number" attributes of each record which is returned in the LDAP search results. When you type in the following field, for example, *Mobile telephoneNumber ipPhone*, you must specify 'Mobile', 'telephoneNumber' and 'ipPhone' fields for each LDAP record.
Display Name **[system/ldap/display_name]**	Specifies the format in which the "name, e.g. "Mike Black" of each returned search result is displayed on the IPPHONE. When you type in the following field, for example:**%sn, %givenName**, the displayed result returned should be "Black, Mike".
Max Hits **[system/ldap/max_hits]**	Specifies the maximum number of entries expected to be sent by the LDAP server (this parameter is sent to the LDAP server).
Sort Result **[system/ldap/sorting_result]**	Sorts the search result by display name on the client side.
system/ldap/predict_text	This parameter appears in the configuration file; however, it is currently not supported.
Search Timeout **[system/ldap/search_timeout]**	The time out value for LDAP search (this parameter is sent to the LDAP server).
system/ldap/ui/use_right_arrow_active_search	This parameter appears in the configuration file; however, it is currently not supported.
system/ldap/lookup_incoming_call	This parameter appears in the configuration file; however, it is currently not supported.
Call Lookup **[system/ldap/call_lookup]**	Performs an LDAP search during call (search the display name for a number).
Country Code **[system/ldap/country_code]**	Defines the country code prefix added for number search.
Area Code **[system/ldap/area_code]**	Defines the area code prefix added for number search.
system/ldap/minimal_name_search_length	Starts to perform an LDAP search after x characters are input.
system/ldap/send_queries_while_typing	Sends an LDAP search each time the user presses a key (all keys with both number and letters).

25.1.2 Loading a Text-based Corporate Directory File

The Configuration file can include a link to a user-defined Corporate Directory file, using the **provisioning/corporate_directory_uri** parameter. This allows you to upload a corporate directory to the phone.

The Corporate Directory file includes a list of contacts and their phone numbers. The file must be a simple text file that can be created using an Excel document and saved as a CSV file.

The syntax of the corporate directory file must be as follows:

```
<full name>,<office>,<home>,<mobile>
```

For example:

```
John Smith,1234,98765432,574685746
```

If not all phone numbers are required, the relevant field must be left empty. For example, in the below directory entry, the home and user-defined numbers are absent:
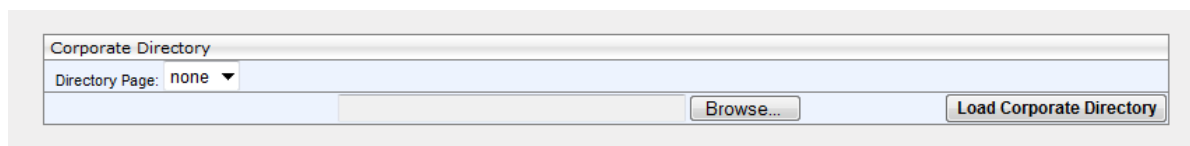
```
John Smith,1234,,574685746
```

➢ **To configure the Corporate Directory:**

■ **Using the Web:**

1. Prepare the TXT-based file as explained above.
2. Access the 'Directory' page (**Configuration** tab > **Personal Settings** menu > **Directory**).
3. Click **Browse** and select the file to upload.
4. Click **Load Corporate Directory**.

Figure 25-2: Corporate Directory Web Field

5. Configure the Corporate Directory settings according to the parameters in the table below, and then click **Submit**.

■ **Using the Configuration File:**

Table 25-2: Provisioning Parameters

Parameter	Description
Note: To add a value to these parameters, enter `provisioning/` followed by the parameter name equals the value (e.g. `provisioning/method=dynamic`).	
provisioning/corporate_directory_uri	The URI for retrieving the corporate directory. The corporate directory must be included in a separate file that can be downloaded to the phone during provisioning. For example: **provisioning/corporate_directory_uri=corporate_dir.txt** **Notes:** ▪ The corporate directory file is downloaded after boot up and periodically. ▪ If the corporate directory file is new, the phone updates the information, does not reboot.
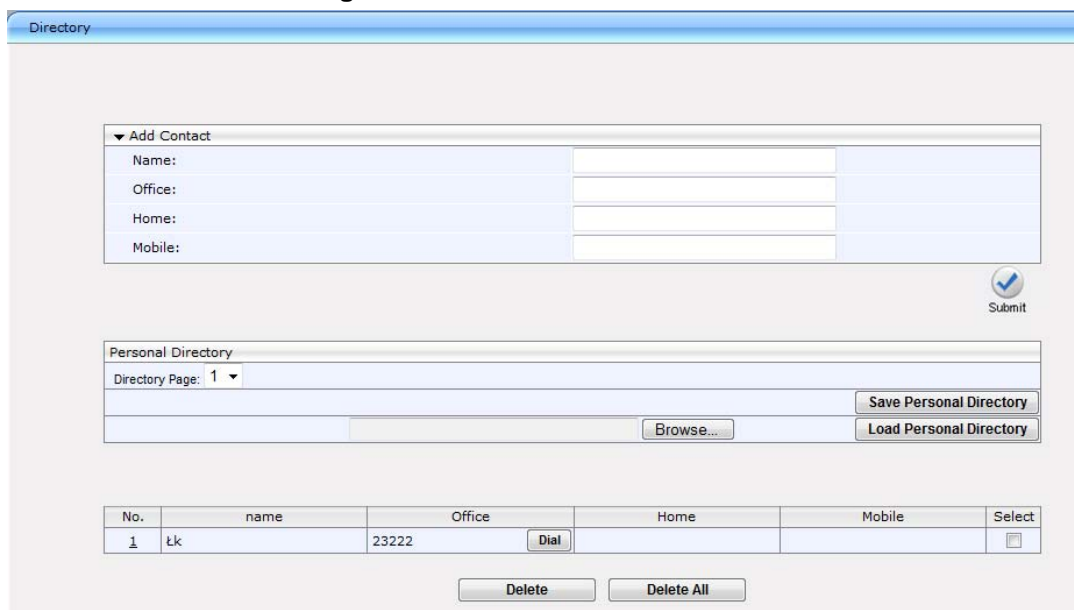
25.2 Local Phone Directory

You can add, edit, or delete directory contacts. A contact's address can be a telephone number, IP address, or domain name. You can also download or upload a personal directory file via the Web interface.

➢ **To add a contact to the phone's directory:**

1. Access the 'Directory' page (**Configuration** tab > **Personal Settings** menu > **Directory**).

Figure 25-3: Add Contact Web Fields

2. Under the **Add Contact** group, define the contact:
3. In the 'Name' field, enter the name of the contact.
4. In the 'Office', 'Home' and/or 'Mobile' fields, enter the contact's telephone numbers. The contact's number can be defined with an IP address or domain name (e.g. <number>@<IP address or domain name>).
5. Click **Submit**; the contact appears in the Directory list at the bottom of the page.

➢ **To edit a contact:**

1. If the contact does not appear in the displayed Directory list, then from the 'Directory Page' drop-down list, select the page in the directory that you want displayed.
2. In the Directory list, click the number that appears in the 'No.' column corresponding to the contact you want to edit; the contact's attributes appear in the **Edit Phone** group above.
3. Edit the contact as required, and then click **Submit**; the contact's new attributes are updated in the Directory list.

➢ **To delete a contact:**

1. In the Directory list, mark the 'Select' check box corresponding to the contact you want to delete.
2. Click **Delete**. (To delete all contacts, click the **Delete All** button.)

26   Speed Dial

Speed Dial can be configured using the Web or Configuration File, as described below.

> **Note:** The phone's speed dials can also be defined in a simple text-based

26.1   Adding a Speed Dial

Adding a Speed Dial can be configured using the Web or Configuration File, as described below.

➢ **To add a speed dial:**

■ **Using the Web:**

    1. Access the 'Speed Dial' page (**Configuration** tab > **Personal Settings** menu > **Speed Dial**).

Figure 26-1: Speed Dial Web Fields

    2. In the 'Number' field corresponding to the phone's Speed Dial key (in the 'Button' column), enter the speed dial number to which you want to assign the Speed Dial key.

    3. Click **Submit**.

■ **Using the Configuration File:**

Table 26-1: Speed Dial Parameters

Parameter Name	Description
provisioning/speed_dial_uri	The URI for retrieving the speed dial list. The speed dial list must be included in a separate file that can be downloaded to the phone during provisioning. For example: **provisioning/speed_dial_uri=speed_dial_list.txt** **Notes:** ▪ The speed dial file is downloaded after boot up and periodically. ▪ If the speed dial file is new, the phone reboots. ▪ For creating a Speed Dial file, see Section 26.3.

26.2 Deleting a Speed Dial

➢ **To delete speed dials, do one of the following:**

- **Deleting selected speed dial entries:** select the 'Delete' check boxes corresponding to the speed dials that you want to delete, and then click **Submit**.
- **All speed dials:** Click **Delete All**, and then at the prompt, click **OK**.
- **To clear (unselect) all selected 'Delete' check boxes:** click **Reset**.

26.3 Saving Speed Dial File Configuration to a File

Once you have configured your Speed Dial in the Web interface, you can save it to a file on your computer. This may be useful for backing up your configuration or for using the same configuration by loading it to another phone.

➢ **To save a Speed Dial:**

1. Access the 'Speed Dial' page (**Configuration** tab > **Personal Settings** menu > **Speed Dial**).
2. Click **Save Speed Dial**.

➢ **To load a Speed Dial:**

1. Access the 'Speed Dial' page (**Configuration** tab > **Personal Settings** menu > **Speed Dial**).
2. Click **Browse….** to select the *.cfg* file.
3. Click **Open**; the selected *.cfg* filename and path appear on the Web interface alongside the **Browse…** button.
4. Click **Load Speed Dial**.

26.4 Creating a Speed Dial File for Configuration File

The Configuration file can include a link to a user-defined Speed Dial file, using the **provisioning/speed_dial_uri** parameter. This allows you to upload speed dial settings to the phone.

The Speed Dial file must include a list of speed dial configurations. The file must be a simple text file that can be created using an Excel document and saved as a CSV file.

The syntax of the speed dial file is as follows:

```
<memory key>,<speed dial phone number>,<type>
```

where:

- *memory key* denotes the speed dial memory key on the phone.
- *speed dial phone number* denotes the phone number that is automatically dialed, when the user presses the speed dial key.
- *type* denotes the Speed Dial feature and must be set to "0".

Below is an example of a Speed Dial file:

```
1,4418,0
2,4403,0
3,039764432,0
4,4391,0
12,1234,0
```

Reader's Notes

Part VII

Security Settings

Reader's Notes

27   Transport Layer Security and Certificate Management

This section describes Transport Layer Security (TLS) and certificate management.

27.1   SIP over TLS Overview

TLS is a cryptographic protocol which provides communication security over the transport layer (TCP). Generally, the TLS protocol uses private and public keys for authentication. The authentication is performed by the certification authority (CA). Full protocol specification is updated in RFC 5246.
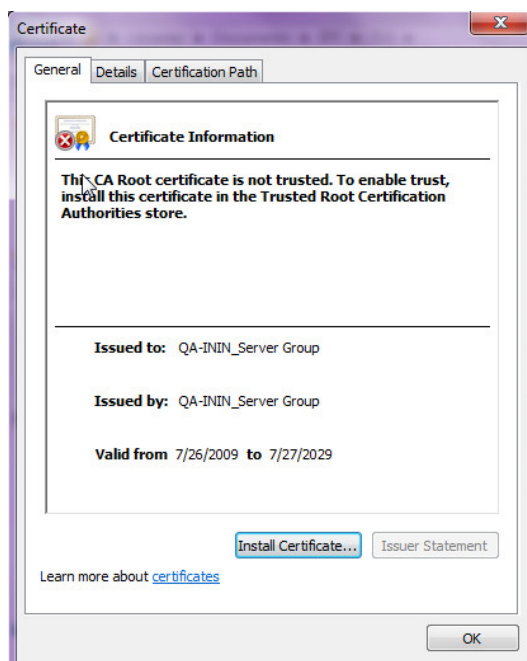
> **Note:** You must obtain the relevant CA, Private and Certificate (Public Key) files from your Certificate Authority (CA).

27.1.1   Obtaining Certificate Authority File

The Certificate Authority (CA) is a body that certifies the ownership of a public key by the name subject of the certificate.

Figure 27-1: Certificate Web Fields

27.1.2   Appending Private and Public Key Data

You must edit the Private file that you received from the CA by appending the Private key and Certificate (Public key) data as shown in the figure below. This action is necessary for the configuration process to retrieve the relevant data. The IP Phone Private key and Certificate data is configured by the same parameter (where each parameter specified below represents a different configuration method (See Section 27.2 on page 183):

■ **Configuration file:** '/provisioning/certificate/private_key_content' and 'provisioning/certificate/private_key_uri'

■ **Web:** 'Private Key and Certificate'

Figure 27-2: Combined Private and Public key Example

```
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQDcgY+Gt//MY/9rK7vy0CFxv0/qEay5zm6H764AT4UDhHbJJRyf
M0OjGpam6I01+RrhuZC47hUtzEdtqTL6dfxs6v3GS88iJkn2RruZ5ZK30i8i9iay
W1I3E3B43wnmL9Db7qqeqRQny1o4WireTvpjfJpnbKyO8Ypj2OmCCi1xewIDAQAB
AoGAc4HCx1U3P7/aGi+sooL4IfePSxO7IRHLwJWC1lLRYIhRGQjBt3tJIPVamVAU
OIOm2zszXkwI+BacDAun0p9ffE1NQaIyihpoTxMThYhQgmpVUdtsz0UqRhMFB+o+
Glf236M2fQr4nTdHvW8OVAhUzGQf7yfR48Ntx6ekjf2B6BECQQD6vSTUApa9UPGD
cPUzEaoCNergUPdM6G72+Gls9NSI73AHYBGA97ba23gah/hBjmjdziF0UxmPAP4Q
KgP1haCXAkEA4SIFJIwg4v8fUIIp9KmhM60RAT+diqLJ90AJPy4x3aLM38YJuRfk
F30ALePuR7MkvuP994GnsfUg9cWjzENuvQJBAO+QN9e4gX1wENCc5Cle/ygNi9O2
iBGbIiolPdU0Nrx+yHLDfvXRt4tzlVUEBFXeUqNZhu01WH4hXJzlB9NVURECQCaT
y8nNcT00dks3YrUX9BWEzGsoWXiOGImToYIACm9uHCkkKDpdS6pysvsqGYSTv/It
4zDsOK4X0QQMT9sKmwkCQAZN7GNJ8QSgwMgwDw4hkmu+GHUXLC6cF68xdUurA2Gc
olCWLrdlpqJSUzp1XHXff/oqEygwjNmPbVujES09c4w=
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIICWzCCAcQCAQgwDQYJKoZIhvcNAQEEBQAwYzEPMA0GA1UEChMGU1ZURVNUMRMw
EQYDVQQHEwpNZXRyb3BvbGlzMREwDwYDVQQIEwhOZXZhZGELMAkGA1UEBhMC
VVMxGzAZBgNVBAMUEnVkaXddAcmFkdmlzaW9uLmNvbTAeFw0wMzA0MTMwNDU0Mzda
Fw0xMzA0MTAwNDU0MzdaMEUxCzAJBgNVBAYTA1VTMREwDwYDVQQIEwhOZXZhZGW9y
azEPMA0GA1UEChMGU1ZURVNUMRIwEAYDVQQDEwkxMjcuMC4wLjEwgZ8wDQYJKoZI
hvcNAQEBBQADgY0AMIGJAoGBANyBj4a3/8xj/2sru/LQIXG/T+oRrLnObofvrgBP
hQOEdsklHJ8zQ6MalqbojTX5GuG5kLjuFS3MR22pMvp1/Gzq/cZLzyImSfZGu5nl
krfSLyL2JrJbUjcTcHjfCeYv0Nvuqp6pFCfLWjhaKt5O+mN8mmdsrI7ximPY6YIK
LXF7AgMBAAGjQjBAMAkGA1UdEwQCMAAwHQYDVR0OBBYEFIIvztAV7cABc8EtVGXA
bgTCKPtdMBQGA1UdEQQNMAuCCWxvY2FsaG9zdDANBgkqhkiG9w0BAQQFAAOBgQCq
31w1LdBxMrifvnFQXePQkGjs95o1sxlh/F3COkyDqmfeUKn1YO4aFhAmL4rkmHFa
BozMWQK19IgS6SgnQR7eB2FWLCp7TGo5sBDYeI/obX1WH0hbtXmeqr6ptB2E+U0Q
XP7hbYFHNZaVebt2M4igjyId4MFCnpq9gw+g7pzZ4A==
-----END CERTIFICATE-----
```

27.2 Configuring TLS

This section describes how to configure TLS.

27.2.1 Configuring TLS using the Configuration file

This section describes how to configure TLS using the Configuration file.

27.2.1.1 Configuring TLS using a URI

This section describes how to configure TLS by directing the configuration to a URI location of the CA Certificate and the Private key files.

> **Note:** Before performing this procedure, ensure that you have uploaded the CA certificate file and the Private key file to an accessible TFTP, FTP, HTTP, or HTTPS server.

➢ **To configure TLS using a URI:**

1. Open the configuration file using a text editor.
2. Specify the full URI of the CA Certificate file. For example:

   `provisioning/certificate/ca_uri= ftp://10.16.2.20/ca_cert.cer`

3. Specify the full URI of the Private key file. For example:

   `provisioning/certificate/private_key_uri= https://auth.com/certfiles/private_keys.cert`

4. Save and close the file.

Table 27-1: SIP-over-TLS Parameters

Parameter	Description
SIP Transport Protocol **[voip/signalling/sip/transport_protocol]**	Specifies the SIP Transport protocol. • If using the 'sip' prefix, set to 'TLS' • If using the 'sips' prefix, set to 'TCP'
TLS Port **[voip/signalling/sip/tls_port]**	Defines the local TLS SIP port for SIP messages. The valid range is 1024 to 65535. The default value is 5061.
/voip/signalling/sip/enable_sips	If signaling protocol is set to TCP and we want to activate TLS, this parameter should be enabled. In this case we will use 'sips' prefix instead of "sip:"
Private Key and Certificate **[provisioning/certificate/private_key_uri]**	The URI for retrieving the private and public keys (combined file). The certificate key must be included in a separate file that can be downloaded to the phone during provisioning. For example: provisioning/certificate/private_key_uri=certificate.cer Notes: ▪ The certificate file is downloaded only after boot up, and not periodically. ▪ If the certificate file is new, the phone reboots.

Parameter	Description
CA Certification **[provisioning/certificate/ca_uri]**	The URI for retrieving the Certificate Authority (CA) key. The CA must be included in a separate file that can be downloaded to the phone during provisioning. For example: provisioning/certificate/ca_uri=ca_cert.cer Notes: ▪ The certificate file is downloaded only after boot up, and not periodically. ▪ If the certificate file is new, the phone reboots.

27.2.1.2 Configuring TLS by Loading File Content

This section describes how to configure TLS by loading the CA certificate file and the Private Key file content to the Configuration file.

> **Note:** Before performing this procedure, ensure that you have uploaded the CA certificate file and the Private Key file to an accessible TFTP, FTP, HTTP, or HTTPS server.

> ➤ **To configure TLS by loading CA Certificate file and the Private Key file content:**

1. Open the configuration file using a text editor.
2. Specify the 'private_key_content' parameter and copy the content of the Private key and Certificate (Public key) file from the appropriate server. For example:

```
/provisioning/certificate/private_key_content=
```

```
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQDcgY+Gt//MY/9rK7vy0CFxv0/qEay5zm6H764AT4UDhHbJJRyf
M0OjGpam6I01+RrhuZC47hUtzEdtqTL6dfxs6v3GS88iJkn2RruZ5ZK30i8i9iay
W1I3E3B43wnmL9Db7qqeqRQny1o4WireTvpjfJpnbKyO8Ypj2OmCCi1xewIDAQAB
AoGAc4HCx1U3P7/aGi+sooL4IfePSxO7IRHLwJWC11LRYIhRGQjBt3tJIPVamVAU
OIOm2zszXkwI+BacDAun0p9ffE1NQaIyihpoTxMThYhQgmpVUdtsz0UqRhMFB+o+
Glf236M2fQr4nTdHvW8OVAhUzGQf7yfR48Ntx6ekjf2B6BECQQD6vSTUApa9UPGD
cPUzEaoCNergUPdM6G72+Gls9NSI73AHYBGA97ba23gah/hBjmjdziF0UxmPAP4Q
KgP1haCXAkEA4SIFJIwg4v8fUIIp9KmhM60RAT+diqLJ90AJPy4x3aLM38YJuRfk
F30ALePuR7MkvuP994GnsfUg9cWjzENuvQJBAO+QN9e4gX1wENCc5Cle/ygNi9O2
iBGbIiolPdU0Nrx+yHLDfvXRt4tzlVUEBFXeUqNZhu01WH4hXJzlB9NVURECQCaT
y8nNcT00dks3YrUX9BWEzGsoWXiOGImToYIACm9uHCkkKDpdS6pysvsqGYSTv/It
4zDsOK4X0QQMT9sKmwkCQAZN7GNJ8QSgwMgwDw4hkmu+GHUXLC6cF68xdUurA2Gc
olCWLrdlpqJSUzp1XHXff/oqEygwjNmPbVujES09c4w=
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIICWzCCAcQCAQgwDQYJKoZIhvcNAQEEBQAwYzEPMA0GA1UEChMGU1ZURVNUMRMw
EQYDVQQHEwpNZXRyb3BvbGlzMREwDwYDVQQIEwhOZXcgWW9yazELMAkGA1UEBhMC
VVMxGzAZBgNVBAMUEnVkaXdAcmFkmlzaW9uLmNvbTAeFw0wMzA0MTMwNDU0Mzda
Fw0xMzA0MTAwNDU0MzdaMEUxCzAJBgNVBAYTA1VTMREwDwYDVQQIEwhOZXcgWW9y
azEPMA0GA1UEChMGU1ZURVNUMRIwEAYDVQQDEwkxMjcuMC4wLjEwgZ8wDQYJKoZI
hvcNAQEBBQADgY0AMIGJAoGBANyBj4a3/8xj/2sru/LQIXG/T+oRrLnObofvrgBP
hQOEdsklHJ8zQ6MalqbojTX5GuG5kLjuFS3MR22pMvp1/Gzq/cZLzyImSfZGu5nl
krfSLyL2JrJbUjcTcHjfCeYv0Nvuqp6pFCfLWjhaKt5O+mN8mmdsrI7ximPY6YIK
LXF7AgMBAAGjQjBAMAkGA1UdEwQCMAAwHQYDVR0OBBYEFIIvztAV7cABc8EtVGXA
bgTCKPtdMBQGA1UdEQQNMAuCCWxvY2FsaG9zdDANBgkqhkiG9w0BAQQFAAOBgQCq
31w1LdBxMrifvnFQXePQkGjs95o1sxlh/F3COkyDqmfeUKn1YO4aFhAmL4rkmHFa
BozMWQK19IgS6SgnQR7eB2FWLCp7TGo5sBDYeI/obX1WH0hbtXmeqr6ptB2E+U0Q
XP7hbYFHNZaVebt2M4igjyId4MFCnpq9gw+g7pzZ4A==
-----END CERTIFICATE-----
```

> **Note:** The PRIVATE KEY and CERTIFICATE file data must be appended as illustrated above.

3. Specify the parameter 'ca_certificate_content' and then copy the content of the CA Certificate file: For example:

`/provisioning/certificate/ca_certificate_content`

```
-----BEGIN CERTIFICATE-----
MIICGjCCAYOgAwIBAgIFFXEymFcwDQYJKoZIhvcNAQEFBQAwSDEQMA4GA1UEChMH
U2VydmVyczEVMBMGA1UECxMMU2VydmVyIEdyb3VwMR0wGwYDVQQDFBRRQS1JTklO
X1NlcnZlciBHcm91cDAeFw0wOTA3MjYwMTUxNTdaFw0yOTA3MjcwMTUxNTdaMEgx
EDAOBgNVBAoTB1NlcnZlcnMxFTATBgNVBAsTDFNlcnZlciBHcm91cDEdMBsGA1UE
AxQUUUUEtSU5JT19TZXJ2ZXIgR3JvdXAwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBAL8FojB//i4HmUBxQMWj+CUEIYcbN57qc+CZT8KeAdisTxTyq5vYsQDh9qlb
WESEyf6Zin8q6RCYoSlQHtcXGpR86ltQqCKFFGaqeXG5GY8HhNZcRP27Kf4RTMNG
bPafS7u4kKps62n4MK1O5bDPwkz1ycML3pQGhbF3IcuLTwdfAgMBAAGjEDAOMAwG
A1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADgYEAJoi5H+8QFt9yC42a+GT2vAB1
ACWyxzxXEWlZ08dFUdD6BgRpaFThYhhtT1o+76eXeqXuy2LitsjNfgi/xfvOM7Tg
Ll/rGoWlSHTmHUB9cB9eu0SSZZ0BPUZVOCrbd4EM65p4QJaxkj9NAql3MSXUecaP
6Mhjcq5Za6qc3tXeZeU=
-----END CERTIFICATE-----
```

4. Save and close the file.

Table 27-2: SIP over TLS File- Encryption File Content Parameters

Parameter	Description
/provisioning/certificate/private_key_content	The content (as string) of the private key file and public key (certificate file) (combined file). You can load the file content here instead of using the provisioning/certificate/private_key_uri parameter
/provisioning/certificate/ca_certificate_content	The content (as string) of the ca_certificate You can load the file content here instead of using the provisioning/certificate/ca_uri parameter

27.2.2 Manually Configuring TLS using the Web

This section describes how to manually configure TLS for a single telephone using the Web.

In this procedure, associate the CA Certificate file and the Private key files to the respective configuration parameter.

Notes:

- Before performing this procedure, ensure that you have saved the CA Certificate file and the Private key files in an accessible location.
- This procedure is generally used for evaluation purposes only.
- For parameter descriptions, see Table 27-2.

➢ **To configure TLS using the Web:**

1. Access the 'Signaling Protocols' page (**Configuration** tab > **Voice Over IP** menu > **Signaling Protocols > SIP General**).

2. From the 'SIP Transport Protocol' drop-down list, select **TLS**.

3. In the 'TLS Port field', enter "5061".

Figure 27-3: TLS Port and CA Certification Web Fields

4. Load the CA certification file (*.cer) using **Browse** and **Load** buttons.

5. Load the combined Private Key and Public Key (*.cer) file using **Browse** and **Load** buttons.

Figure 27-4: Private and Public Key Web Fields

6. Click **Submit**.

28   Using the Encryption Tool

The following describes how to use the Encryption tool.

28.1   Encrypting Configuration Files

This procedure describes how to encrypt the Configuration file. For example, you may wish to encrypt the configuration file when it is send over an unsecure network.

➢ **To encrypt the configuration file:**

■   At the command line prompt, specify the following:

```
encryption_tool.exe –f <filename>.cfg
```

where *<file name>*.cfg specifies the name of the Configuration file that you wish to encrypt.

Once the Configuration file is encrypted, it receives the suffix '.cfx' (e.g. Conf.cfx). This is the file that you should specify in the 'Configuration URL' and the 'Dynamic Configuration URL' fields when performing automatic provisioning (see Part II 'Automatic Provisioning').

28.2   Encrypting Passwords in Configuration File

This procedure below describes how to encrypt IP phone passwords used in the configuration process, for example, the 'System' password and the 'SIP Authentication' password.

➢ **To encrypt passwords:**

1.   At the command line prompt, specify the following:

```
encryption_tool.exe –s <password_string>
```

where *<password_string>* specifies the string of the password that you wish to encrypt.

Once the password is encrypted, a string is generated with the following syntax:

```
{"<encrypted_string>"}
```

For example:

```
{"0qrNRpSJ6aE="}
```

2.   Copy the generated string (including the {" "}) with the syntax specified above to the relevant parameter in the Configuration file.

For example, if you encrypted the SIP authentication password, the following is displayed in the relevant line in the configuration file:

```
voip/line/0/auth_password={"0qrNRpSJ6aE="}
```

> **Note:** It is recommended to encrypt the System password using this procedure. If you choose not to do so, then the System password is by default encrypted using MD5.

Reader's Notes

29   Secure Real-time Transport Protocol

Secure Real-time Transport Protocol (SRTP) is a protocol that allows encryption for RTP data. Since the RTP encryption key is delivered via SIP, this feature is relevant only when SIP transport is secured. Therefore, when using this feature you also need to use SIP over TLS.

SRTP can be configured using the Web or Configuration File, as described below.

➢ **To configure SRTP:**

■ **Using the Web:**

1. Access the 'Media Streaming' page (**Configuration** tab > **Voice Over IP** menu > **Media Streaming**).

Figure 29-1: Enabling SRTP Web Fields

2. Configure the SRTP settings according to the parameters in the table below, and then click **Submit**.

■ **Using the Configuration File:**

Table 29-1: SRTP Parameters

Parameter	Description
Enable SRTP Encryption and Authentication **[voip/media/srtp/enabled]**	Enables secured RTP (SRTP). ▪ **[0]** Disable (default) ▪ **[1]** Enable
Method **[voip/media/srtp/method]**	The SRTP encryption method. ▪ **[AES_CM_128_HMAC_SHA1_32]** (default) ▪ **[AES_CM_128_HMAC_SHA1_80]** ▪ **[AES_CM_128_ALL_METHODS]**
ARIA **[voip/media/srtp/aria_support_enabled]**	Adds the ARIA encryption method to the list of supported encryption the phone publishes. ▪ **[0]** Disable (default) ▪ **[1]** Enable
/voip/media/srtp/use_MKI	Defines the Master Key Index from SDP.
/voip/media/srtp/MKI_length	Defines the Maximum length of the Master Key Index.

Reader's Notes

30   Configuring 802.1x

802.1X is an IEEE Standard for port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

30.1   Configuring 802.1x using Phone User Interface

The procedures for configuring 802.1x on the 310HD IP Phone and 320HD IP Phone using the Phone User Interface, are described below.

30.1.1   310HD IP Phone

The procedure below describes how to configure the 802.1x settings using the 310HD IP Phone.

➢ **To configure 802.1x:**

1. Access the Settings screen (MENU key > **Administration** menu > **Network Settings** submenu).

```
┌─────────────────────┐       ┌─────────────────────┐
│  Status             │       │  Network Settings   │
│  Administration     │  ──▶  │  SIP Accounts       │
└─────────────────────┘       └─────────────────────┘
```

```
                    ┌─────────────────────┐
                    │  LAN Conn. Type     │
               ──▶  │  802.1X Settings    │
                    └─────────────────────┘
```

The following screen appears:

```
                    ┌─────────────────────┐
                    │  Disabled           │
               ──▶  │  EAP-MD5            │
                    └─────────────────────┘
```
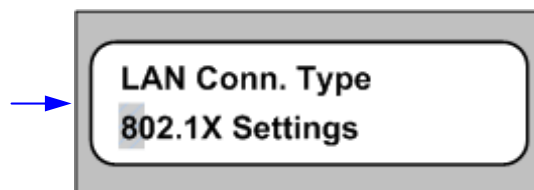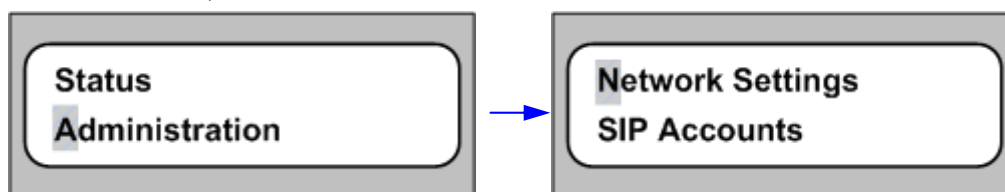
2. Using the ▲ and ▼ Navigation keys, choose one of the following IP addressing schemes:
    - Disabled – disables the 802.1x feature
    - EAP-MD5 – see Section 30.1.1.1
    - EAP-TLS – see Section 30.1.1.2

30.1.1.1 EAP-MD5 Mode

This option enables the 802.1x feature in EAP-MD5 mode. In this mode, define the following:

■ **Identity:** Defines the User ID.

■ **MD5 Password:** Defines the Password (optional).

```
Identity
MD5 Password
```

➢ **To enable the 802.1x feature in EAP-MD5 mode:**

    1. Enter the Identity (User ID).

    2. Enter the MD5 Password (optional).

    3. Press the left ◀ Navigation key until you are prompted to save settings, as shown below:

```
Save Settings?
[✱] Yes        [ ] No
```

    4. Select the **Yes** option (using the ◀ and ▶ Navigation keys), and then press the ENTER key; the settings are saved.

30.1.1.2 EAP-TLS Mode

This option enables the 802.1x feature in EAP-TLS mode. In this mode, define the following:

```
Identity
Root Cert. URL
```
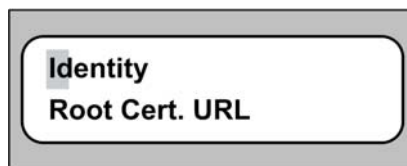
➢ **To enable the 802.1x feature in EAP-TLS mode**

1. Define the following:
    ♦ **Identity:** Enables the User ID.
    ♦ **Root Cert. URL:** Enables the full URL of the file which contains the root certification file.
    ♦ **Trusted Cert URL:** Enables the full URL of the file which contains the trusted certification file.
    ♦ **Local Cert URL:** Enables the full URL of the file which contains the local certification file.
    ♦ **Private key URL:** Enables the full URL of the file which contains the private key file.
    ♦ **Private key Password:** (Optional) In case the private key file is encrypted, input the password to decrypt the file.
2. Press the left ◀ Navigation key until you are prompted to save settings, as shown below:

```
Save Settings?
[*] Yes        [ ] No
```
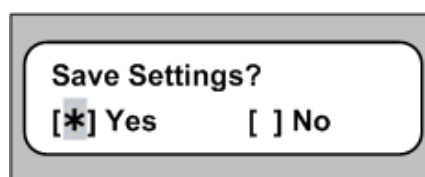
3. Select the **Yes** option (using the ◀ and ▶ Navigation keys), and then press the ENTER key; the settings are saved.

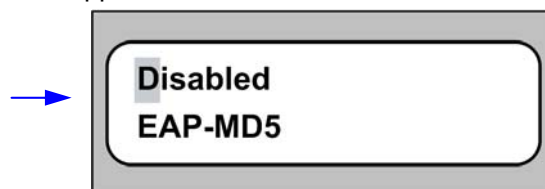## 30.1.2   320HD IP Phone

The procedure below describes how to configure the 802.1x settings using the 320HD IP Phone.

➢ **To configure 802.1x:**

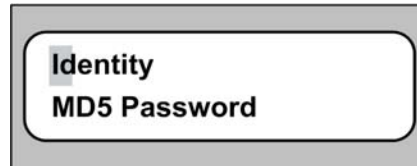1. Access the Settings screen (MENU key > **Administration** menu > **Network Settings** submenu).

```
Menu                    00:48        Administration         02:31
  3. Speed Dial            ▲          1. Network Settings
  4. Settings                         2. SIP Accounts
  5. Status                           3. Restore Defaults
  6. Administration                   4. Restart
Select              Back            Select             Back
```

The following screen appears:

```
Settings                22:37
  1. LAN Connection Type
  2. 802.1X Settings


Select              Back
```
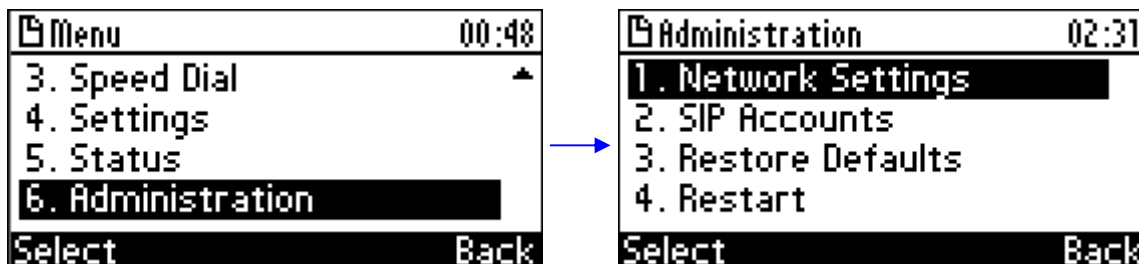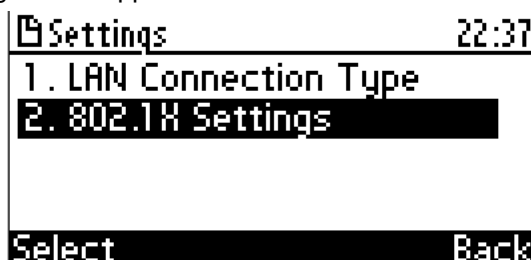
2. Using the ▲ and ▼ Navigation keys, choose **802.1X Settings**, and then press the **Select** softkey; the following screen appears:
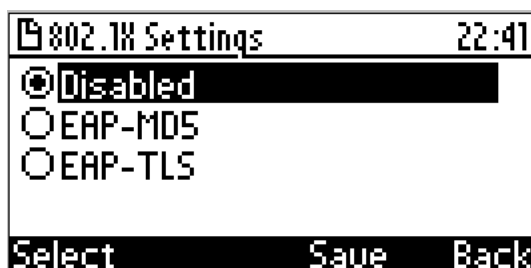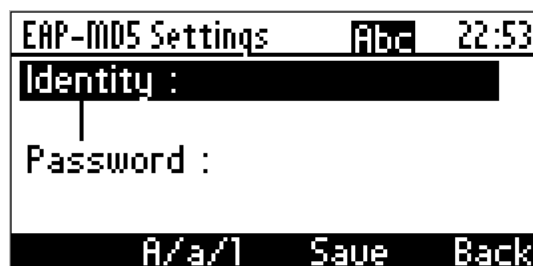
```
802.1X Settings         22:41
  ◉ Disabled
  ○ EAP-MD5
  ○ EAP-TLS

Select          Save    Back
```

3. Using the ▲ and ▼ Navigation keys, choose one of the following IP addressing schemes:

   - Disabled – disables the 802.1x feature
   - EAP-MD5 – see Section 30.1.3.1
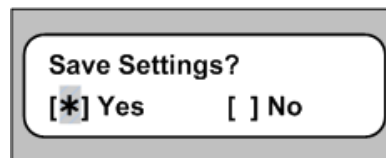   - EAP-TLS - see Section 30.1.3.2

30.1.2.1 EAP-MD5 Mode

The procedure for configuring EAP-MD5 mode for 802.1x is described below.

➢ **To configure EAP-MD5 mode for 802.1x:**

1. Using the ▲ and ▼ Navigation keys, choose the **EAP-MD5** option, and then press **Select** and then **Edit**; the following screen appears:

```
EAP-MD5 Settings    Abc   22:53
Identity :
    |
Password :


           A/a/1    Save    Back
```

2. Enter the following information:
    *   **Identity:** User ID
    *   **Password:** MD5 password (optional)
3. Press the **Save** softkey; a message appears notifying you that the phone will restart.
4. Press **Apply**.

30.1.2.2 EAP-TLS Mode

The procedure for configuring EAP-TLS mode for 802.1x is described below.

➢ **To configure EAP-TLS mode for 802.1x:**

1. Using the ▲ and ▼ Navigation keys, choose the **EAP-MD5** option, and then press **Select** and then **Edit**; the following screen appears:

```
EAP-TLS Settings    Abc   23:04
Identity :
    |
Root Certificate URL :
                          ▼
           A/a/1    Save    Back
```

2. Enter the following information:
    *   **Identity:** user ID.
    *   **Root Certificate URL:** full URL of the file which contains root certification file.
    *   **Trusted Certificate URL:** full URL of the file which contains trusted certification file.
    *   **Local Certificate URL:** full URL of the file which contains local certification file.
    *   **Private Key URL:** full URL of the file which contains the private key file.
    *   **Private key Password:** (option) In case the private key file is encrypted you should input the password to decrypt the file)
3. Press the **Save** softkey; a message appears notifying you that the phone will restart.
4. Press **Apply**.

30.1.3   420HD IP Phone

Configuring 802.1x settings using the 420HD IP Phone is identical to configuring 802.1x settings using the 320HD IP Phone.

➢ **To configure 802.1x:**

1. Access the Settings screen (MENU key > **Administration** menu > **Network Settings** submenu).

```
Administration                         Settings
 1. Network Settings                    1. LAN Connection Type
 2. SIP Accounts                        2. 802.1X Settings
Select                    Back         Select                    Back
```

2. Press the navigation control's lower rim to navigate to **802.1X Settings** and then press the **Select** softkey.

```
802.1X Settings
 ⦿ Disabled
 ○ EAP-MD5
Select              Save     Back
```

3. Press the navigation control's lower or upper rim to navigate to and select either:
   - Disabled – disables the 802.1x feature
   - EAP-MD5 – see Section 30.1.3.1
   - EAP-TLS - see Section 30.1.3.2

30.1.3.1 EAP-MD5 Mode

The procedure for configuring EAP-MD5 mode for 802.1x is described below.

➢ **To configure EAP-MD5 mode for 802.1x:**

1. Press the navigation control's lower rim to navigate to the **EAP-MD5** option and then press **Select** and **Edit**:

```
EAP-MD5 Settings        Abc
 Identity :
      |
            A/a/1     Save     Back
```

2. Enter the following information:
   - **Identity:** User ID
   - **Password:** MD5 password (optional)

3. Press the **Save** softkey; a message appears notifying you that the phone will restart.

4. Press **Apply**.

30.1.3.2 EAP-TLS Mode

The procedure for configuring EAP-TLS mode for 802.1x is described below.

> ➢ **To configure EAP-TLS mode for 802.1x:**

1. Press the navigation control's lower rim to navigate to the **EAP-TLS** option and press **Select** and then **Edit**; this screen appears:

```
EAP-TLS Settings      Abc
Identity :

|

         A/a/1    Save   Back
```
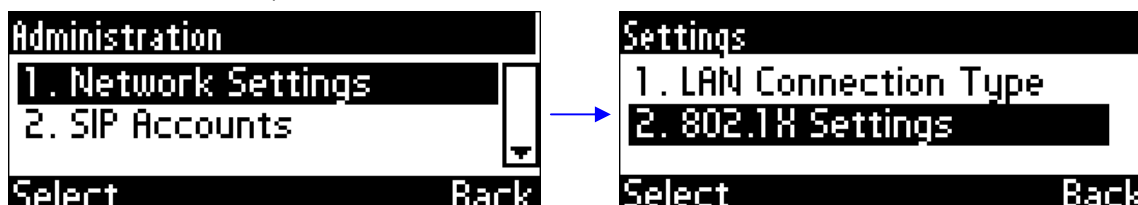
2. Enter the following information:
- **Identity:** user ID.
- **Root Certificate URL:** full URL of the file which contains root certification file.
- **Trusted Certificate URL:** full URL of the file which contains trusted certification file.
- **Local Certificate URL:** full URL of the file which contains local certification file.
- **Private Key URL:** full URL of the file which contains the private key file.
- **Private key Password:** (option) In case the private key file is encrypted you should input the password to decrypt the file)

3. Press the **Save** softkey; a message appears notifying you that the phone will restart.

4. Press **Apply**.

30.2 Configuring 802.1x using Web and Configuration File

802.1x can be configured using the Web or Configuration File, as described below.

30.2.1 EAP MD5 Mode

This section describes how to configure 802.1x settings for EAP-MD5.

➢ **To configure the phone's 802.1x settings for EAP-MD5:**

■ **Using the Web:**

1. Access the '802.1X Settings' page (**Network Connections** > **802.1X Settings**).

Figure 30-1: EAP MD5 Web Fields

2. Configure the 802.1x settings according to the parameters in the table below, and then click **Submit**.

■ **Using the Configuration File:**

Table 30-1: EAP MD5 Parameters

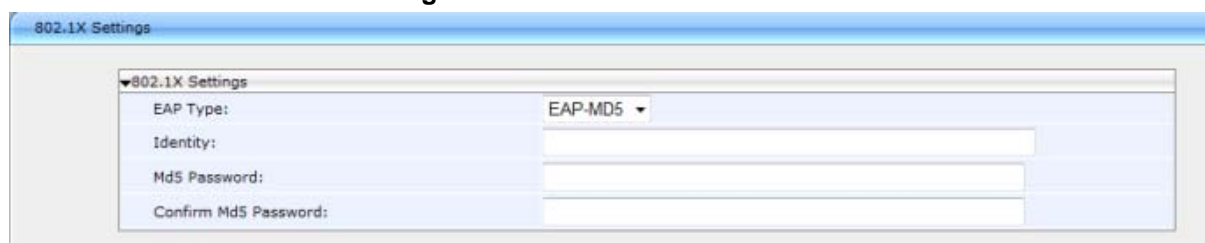| Parameter	Description
EAP Type **[/network/lan/_802_1x/eap_type]**	Sets 802.1x Extensible Authentication Protocol mode. [Disable] = Disables the use of 802.1x [EAP_MD5]=Authentication is implemented by user name and password (Password is optional). [EAP_TLS]= Authentication is implemented by Certificate, Client Certificate and Client Private Key.
Identity **[/network/lan/_802_1x/md5_identity]**	User ID for md5 mode.
MD5 password **[/network/lan/_802_1x/md5_password]**	Password for md5 mode. (Leave blank if no password).

30.2.2 EAP TLS Mode

This section describes how to configure phone's 802.1x settings for EAP-TLS.

➢ **To configure the phone's 802.1x settings for EAP-TLS:**

■ **Using the Web:**

1. Access the '802.1X Settings' page (**Network Settings** > **802.1X Settings**).

Figure 30-2: EAP TLS Web Fields

▼802.1X Settings	
EAP Type:	EAP-TLS ▼
Identity:	
Root and Intermediate Certificate Filename:	
Trusted Certificate Filename:	
Local Certificate Filename:	
Private Key Filename:	
Private Key Password:	
Confirm Private Key Password:	

2. Configure the 802.1x settings according to the parameters in the table below, and then click **Submit**.

■ **Using the Configuration File:**

Table 30-2: EAP TLS Parameters

Parameter	Description
Identity **/network/lan/_802_1x/tls_identity**	Identity for TLS mode. (optional)
Root and Intermediate Certificate Filename **[/network/lan/_802_1x/root_ca_url]**	URL for the file that contains root and intermediate Certificate.
Trusted Certificate Filename **[/network/lan/_802_1x/trust_ca_url]**	URL for the file that contains a trusted Certificate.
Local Certificate Filename **[/network/lan/_802_1x/local_ca_url]**	URL for the file that contains a local Certificate.
Private Key Filename **[/network/lan/_802_1x/private_key_url**	URL for file that contains the private key.
Private Key Password **[/network/lan/_802_1x/private_key_password]**	Optional: If the file that contains the private key is encrypted, then this is the password for decryption.

Reader's Notes

31   HTTPS Management

This section describes HTTPS secure management.
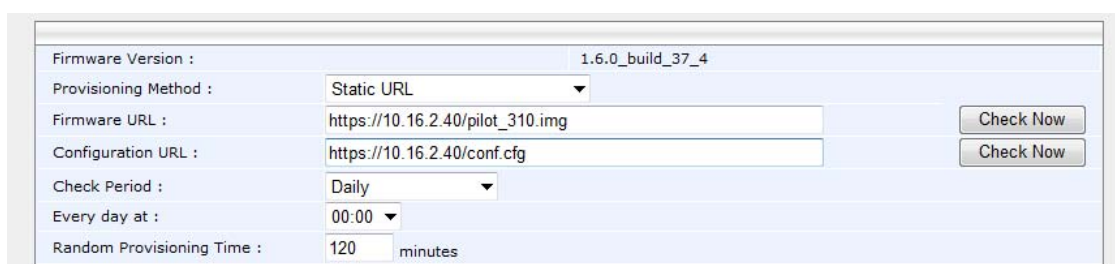
31.1   Web Interface

You can choose to access the IP Phone Web interface using HTTPS for example, "https://10.16.2.40".

31.2   Secure Provisioning

You can load firmware and configuration files to the IP phone from an HTTPS server as specified in the Firmware and Configuration URLs (displayed in the example Automatic Provisioning screen below).

Figure 30-1: Automatic Provisioning Web Fields

Firmware Version :	1.6.0_build_37_4	
Provisioning Method :	Static URL	
Firmware URL :	https://10.16.2.40/pilot_310.img	Check Now
Configuration URL :	https://10.16.2.40/conf.cfg	Check Now
Check Period :	Daily	
Every day at :	00:00	
Random Provisioning Time :	120 minutes	

> **Note:** To implement secure provisioning using HTTPS, the HTTPS server on the far end (from where you are loading the files) must also support HTTPS.

Reader's Notes

Part VIII

Maintenance

Reader's Notes

32 Changing User Login Credentials

You can change the phone's login user name and password. This is the login required for accessing the Web interface and the **Administration** menu of the phone's LCD screen. The default user name and password is "admin" and "1234" respectively.

User Login Credentials can be changed using the Web or Configuration File, as described below.

➢ **To change the login username and password:**

■ **Using the Web:**

1. Access the 'System Authorization' page (**Management** tab > **Administration** menu > **Users**).

Figure 32-1: System Authorization Web Fields

2. In the 'Username' field, enter a user name.
3. In the 'Password' field, enter a new password, and then in the 'Confirm Password' field, re-enter this new password.
4. Click **Submit**; a confirmation box appears.
5. Click **OK**.

■ **Using the Configuration File:**

Table 32-1: Username and Password Parameters

Parameter	Description
Note: To add a value to these parameters, enter **system/** followed by the parameter name, equal sign and then the value (e.g. `system/user_name=admin`).	
Username **[system/user_name]**	The phone user name. The default value is admin. **Note:** This parameter is applicable only to the Web and Telnet interfaces.
Password **[system/password]**	The encrypted phone password. The default value is 1234. To generate an encrypted password, see Section 28 on page 189. **Note:** This parameter is applicable only to the Web and Telnet interfaces, and LCD display.

Reader's Notes

33   Restarting Phones

The 310HD, 320HD and 420HD IP Phones can be restarted using the phone user interface or the Web.

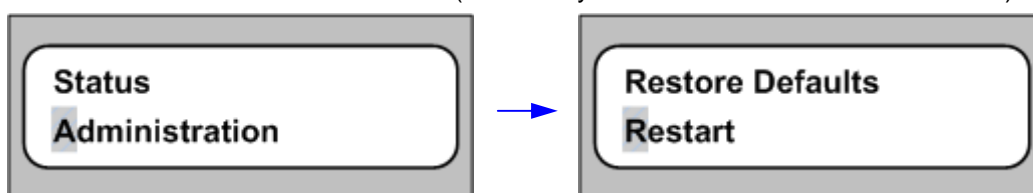## 33.1   Restarting Phone using Phone User Interface

The procedures below describe how to restart the phone using the phone user interface.

33.1.1   310HD IP Phone

The procedure below describes how to restart the 310HD IP Phone using the phone user interface.

➢ **To restart the 310HD IP Phone:**

1. Select the **Restart** submenu (**MENU** key > **Administration** menu > **Restart**):

A confirmation message appears, prompting you to confirm phone reset:
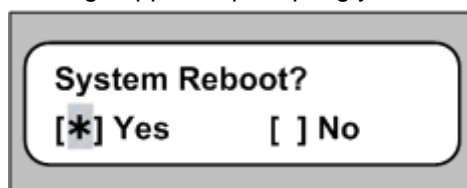
2. Select the **Yes** option (using the ◄ and ► Navigation keys), and then press the ENTER key; the phone resets.

⚠️ **Notes:**

- You can remotely reset the phone by sending a SIP NOTIFY message to the phone with the "check-sync" or "resync" events. This reset allows for graceful shutdown, whereby the phone resets only when there are no calls, i.e., when the phone is in idle state.

- Upon receipt of a "check-sync" or "resync" message, the phone immediately retrieves the configuration file and reboots if a new configuration is provided.

- The phone can be configured to reboot even if no configuration update is required.

- The phone supports the optional "reboot" parameter located in the Event header of the NOTIFY message (e.g. Event: check-sync;reboot=true, Event: resync;reboot=false, etc.).

- When set to "false" or not present, the phone retrieves its new configuration file and reboots only if the configuration was updated.

- When set to "true", the phone reboots without trying to get the configuration file.

33.2   Restarting Phone using Web

You can use the Web interface to restart your phone.

➢ **To restart the phone:**

1.   Access the 'Restart System' page (**Management** tab > **Administration** menu > **Restart System**).

Figure 33-1: Restart System Web Fields

Restart system	Restart

2.   Click the **Restart** button; a confirmation box appears prompting you to confirm.

Figure 33-2: Confirmation Box

3.   Click **OK**.

310HD, 320HD and 420HD IP Phones
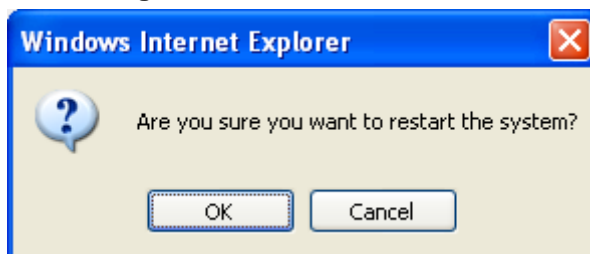
Reader's Notes

34   Restoring Phone Defaults

Phone default settings can be restored using the phone or Web interface.

34.1   Restoring Factory Defaults using Phone Interface

The procedures for restoring factory defaults using the IP Phone user interface are described below.

34.1.1   310HD IP Phone

The procedures below describe how to restore the 310HD IP Phone factory defaults using the phone.

> ➢   **To restore the 310HD IP Phone to default settings:**

1. Select the **Restore Defaults** submenu (**MENU** key > **Administration** menu > **Restore Defaults**):
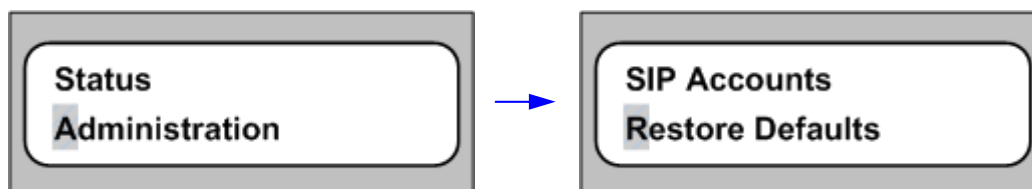
A confirmation message appears, prompting you to confirm factory reset:
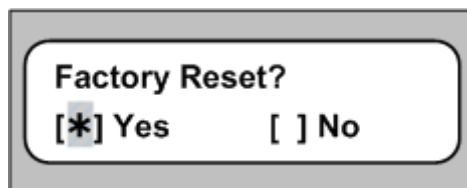
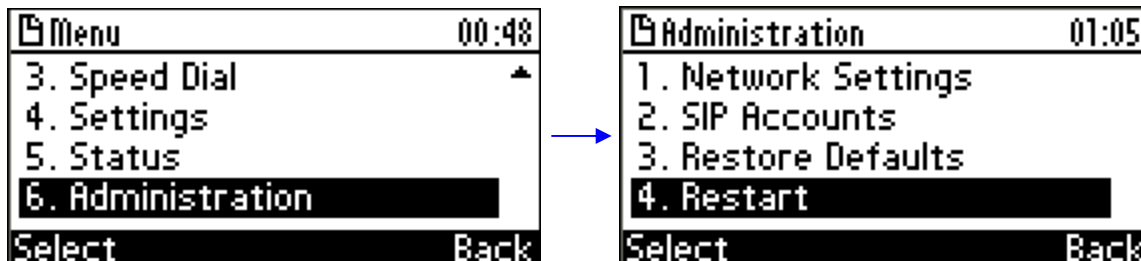2. Select the **Yes** option (using the ◀ and ▶ Navigation keys), and then press the ENTER key; the phone is restored to factory defaults.

⚠	**Note:**	You can also restore the phone to default settings by using a hard-coded sequence of keys on the phone's keypad. To do this:
		• Unplug the power cable from the phone.
		• Press the following keys at the same time - ▶ Navigation key, MENU and ENTER.
		• While pressing the above keys, plug the power cable into the phone. Once the power is connected, keep pressing the keys for five seconds and then release the keys.

34.1.2 320HD IP Phone

The procedure below describes how to restore the 320HD IP Phone factory defaults using the phone.

➢ **To restore the phone to default settings:**

1. Access the **Restore Defaults** submenu (**MENU** key > **Administration** menu > **Restore Defaults**).

Menu 00:48	Administration 00:49
3. Speed Dial ▲	1. Network Settings
4. Settings	2. SIP Accounts
5. Status	3. Restore Defaults
6. Administration	4. Restart
Select Back	Select Back

A warning message appears, requesting you to confirm:

```
 Administration          02:41AM
┌─────────────────────────────┐
│         Warning             │
│     Restore settings?       │
└─────────────────────────────┘
 6. Restart
 Yes                       No
```
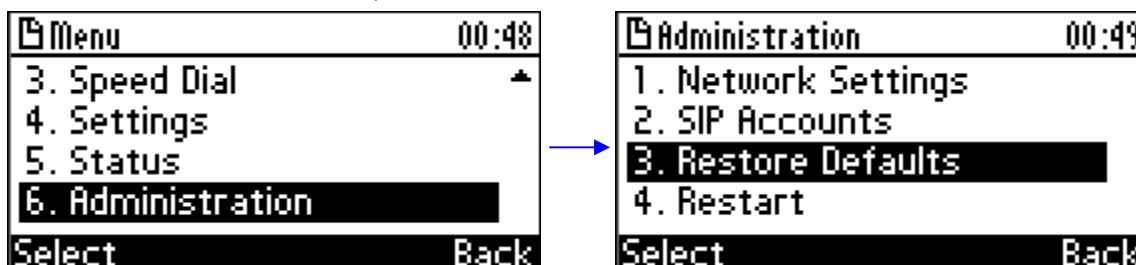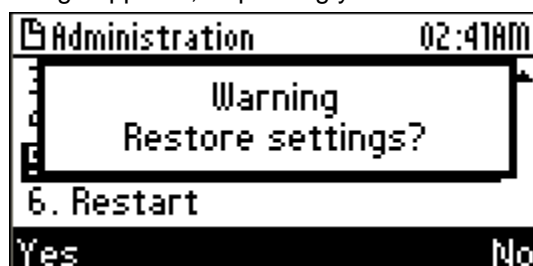
2. Press the **Yes** softkey to confirm reset to defaults or **No** if you want to cancel.

⚠️ **Notes:** You can also restore the phone to default settings by using a hard-coded sequence of keys on the phone's keypad. To do this:

- Unplug the power cable from the phone.
- Press the ◄ and ▼ Navigation keys and the ENTER key all together.
- While pressing the above keys, plug the power cable into the phone. Once the power is connected, keep pressing the keys for five seconds and then release keys.

34.1.3 420HD IP Phone

The procedure for restoring the 420HD IP Phone factory defaults is identical to that for the 320HD IP Phone.

➢ **To restore the phone to default settings:**

1. Access the **Restore Defaults** submenu (**MENU** key > **Administration** menu > **Restore Defaults**).
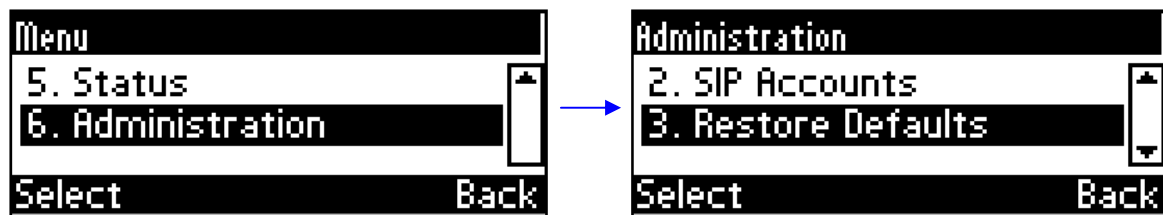
2.   Press the **Select** softkey; a warning message appears requesting you to confirm:

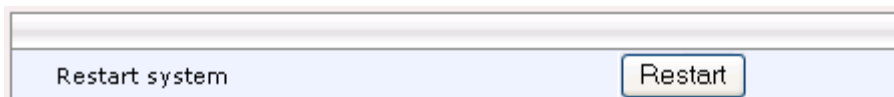3.   Press the **Yes** softkey to confirm reset to defaults or **No** if you want to cancel.

> **Notes:** You can also restore the phone to default settings by using a hard-coded sequence of keys on the phone's keypad. To do this:
>
> - Unplug the power cable from the phone.
> - Press the OK and the MENU key together.
> - Plug the power cable into the phone and keep the keys pressed for five seconds.

34.2   Restoring Factory Defaults using the Web

You can restore all your phone's settings to factory default settings using the Web.

➢   **To restore the phone to factory defaults:**

1.   Access the 'Restore Defaults' page (**Management** tab > **Administration** menu > **Restore Defaults**).

Figure 34-1: Restore Defaults Web Fields

2.   Click the **Submit** button; a confirmation box appears prompting you to confirm.

Figure 34-2: Submit Confirmation Box
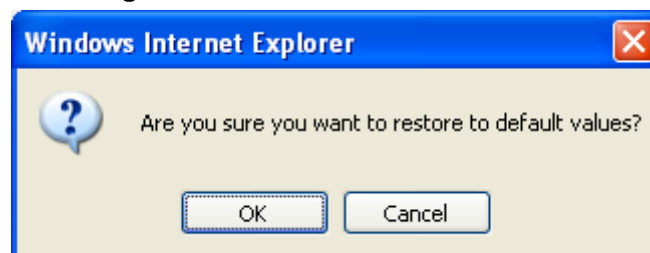
3.   Click **OK**.

Reader's Notes

Part IX

Status and Monitoring

Reader's Notes

35   Viewing Network Status

This section describes how to view the network status using the Web interface.

35.1   LAN Status

The following describes how to view LAN status information.

➢ **To view LAN status information:**

■ Access the 'Network Status' page (**Status & Diagnostics** tab > **System Status** menu > **Network Status**).

Figure 35-1: LAN Information Web Fields

LAN Information	
Type:	DHCP Client
IP Address:	10.16.2.162
Subnet Mask:	255.255.0.0
Default Gateway Address:	10.16.0.1
Primary DNS:	10.1.1.11
Secondary DNS:	10.1.1.10
MAC Address:	00:90:8F:1E:DB:3E

35.2 Port Status

The following describes how to view the Port Mode status.

➢ **To view Port Mode status:**

■ Access the 'Network Status' page (**Status & Diagnostics** tab > **System Status** menu > **Network Status**).

Figure 35-2: Port Mode Status Web Fields

Port Mode Status		
Attribute	**LAN Port**	**PC Port**
Link State:	Up	Down
Negotiation:	Automatic	Automatic
Speed:	100Mbps	N/A
Duplex:	Full	N/A

35.3   802.1x Status

The following describes how to view 802.1x status.

➢ **To view 802.1x status:**

■ Access the 'Network Status' page (**Status & Diagnostics** tab > **System Status** menu > **Network Status**).

Figure 35-3: 802.1X Status Web Fields

802.1X Status	
EAP Type:	EAP-TLS
Status:	Failure: No certificates

Reader's Notes

36   Viewing VoIP Status

The following describes how to view VoIP status using the Web interface.
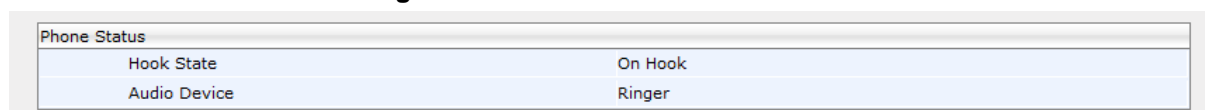
36.1   Phone Status

This section describes how to view the phone status.

➢ **To view the phone status:**

■   Access the 'Network Status' page (**Status & Diagnostics** tab > **System Status** menu > **VoIP Status**).

Figure 36-1: Phone Status Web Fields

Phone Status	
Hook State	On Hook
Audio Device	Ringer

36.2   Line Status

This section describes how to view the line status.

> ➢ **To view the line status:**

■ Access the 'Network Status' page (**Status & Diagnostics** tab > **System Status** menu > **VoIP Status**).

Figure 36-2: Line Status Web Fields

Line Status	
Line Number	Line 1
SIP Registration	Registered
DnD	On
Mute	Off
Forward State	Disabled
Forward Destination	N/A

36.3   Current Call Information

The Web interface displays call information of a currently established call.

➢   **To view the line information:**

■   Access the 'Network Status' page (**Status & Diagnostics** tab > **System Status** menu > **VoIP Status**).

Figure 36-3: Current Call Information Web Fields

Line 1 Call Information	
Call Number	Call 1
Call State	Connected
Origin	Outgoing
Remote Number	569
Remote ID	Sue Lee
Duration	00:00:22
Codec	G722
Packets Sent	825
Packets Received	826
Bytes Sent	132000
Bytes Received	132160
Packets Lost	0
Fraction Lost	0.0%
Jitter	1
Round Trip Delay	22

Reader's Notes

37   Viewing Call History

You can view a list of received calls, missed calls, and dialed numbers. The call duration of the received and dialed calls is also displayed.

➢   **To view call history log:**

1.   Access the 'Call History' page (**Status & Diagnostics** tab > **History** menu > **Call History**).

Figure 37-1: Call History Web Fields

2.   From the 'Type' drop-down list, select the type of call history (i.e., missed calls, received calls, and dialed numbers) that you want to view; the table lists the call history according to the chosen call history type.

3.   You can delete a logged call history entry, by selecting the 'Delete' check box corresponding to the entry that you want to delete, and then clicking the **Delete** button.

Reader's Notes

38   Viewing Phone Version Number

You can view the phone firmware version number via the Web or on the phone itself.

38.1   Viewing Phone Version Number using the Web

You can view the phone's model name as well as the firmware version currently running on the phone.

➢ **To view the phone's model and version number:**

■ Access the 'System Information' page (**Status & Diagnostics** tab > **System Information** menu > **Versions**).

Figure 38-1: System Information Web Fields (for example 310HD Model)

Model Name	310HD
Firmware Version	1.4.1_build_32
Release Date	21 December 2010 18:55:01

38.2 Viewing Firmware Version using Phone Interface

You can view the phone's model number and firmware version on the phone.

38.2.1 310HD IP Phone

The procedures below describe how to view the 310HD IP Phone's model number and firmware version on the phone.

➢ **To view the phone's firmware version:**

1. From the idle screen, press the MENU key, select the **Status** menu, and then the **Firmware Version** submenu.
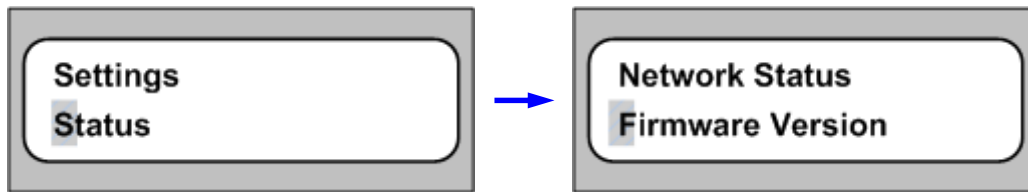
The following screen appears:

2. Press the ENTER key; the phone's model and firmware version is displayed.
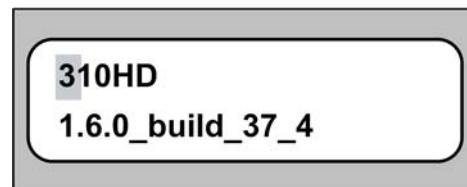
38.2.2 320HD IP Phone

The procedures below describe how to view the 320HD IP Phone's model type, firmware version, and configuration file version.

➢ **To view the phone's firmware version:**

1. Access the Software Versions screen (MENU key > **Status** menu > **Firmware Version**).
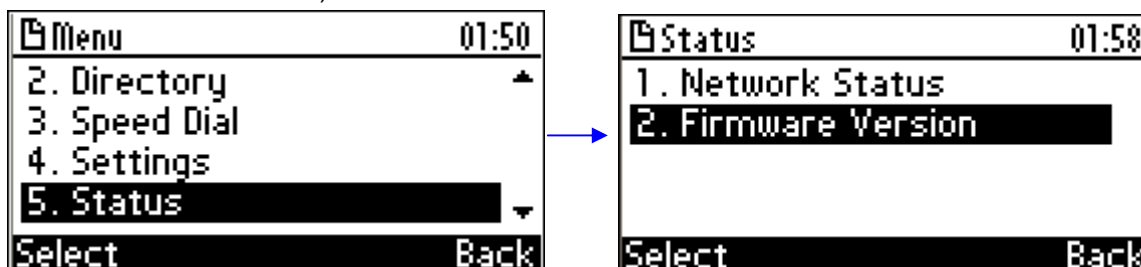
```
┌──────────────────────────┐     ┌──────────────────────────┐
│ 🗋Menu          01:50    │     │ 🗋Status        01:58    │
│  2. Directory        ▲   │     │  1. Network Status       │
│  3. Speed Dial           │ ──► │ █2. Firmware Version███  │
│  4. Settings             │     │                          │
│ █5. Status██████████  ▼  │     │                          │
│ Select         Back      │     │ Select         Back      │
└──────────────────────────┘     └──────────────────────────┘
```

2. The following screen appears, displaying the phone model and the firmware version currently running on the phone:

```
┌──────────────────────────┐
│ 🗋Status        01:16    │
│   ┌────────────────────┐ │
│   │      320HD         │ │
│   │  Firmware Version  │ │
│   │  1.6.0_build_37_4  │ │
│   └────────────────────┘ │
│                          │
│ ████████████████   Back  │
└──────────────────────────┘
```

38.2.3   420HD IP Phone

The procedures below describe how to view the 420HD IP Phone's model type, firmware version, and configuration file version.

> ➢ **To view the phone's firmware version:**

1. Access the Firmware Version screen (MENU key > **Status** menu > **Firmware Version**).
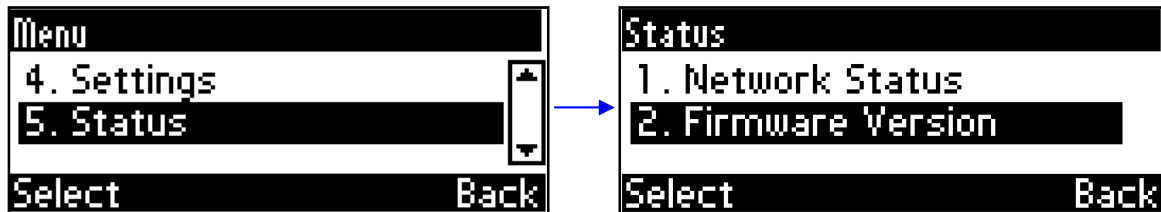
```
┌──────────────────────┐        ┌──────────────────────┐
│Menu                  │        │Status                │
│ 4. Settings          │  ──→   │ 1. Network Status    │
│ 5. Status            │        │ 2. Firmware Version  │
│Select           Back │        │Select           Back │
└──────────────────────┘        └──────────────────────┘
```

2. The following screen appears, displaying the phone model and the firmware version currently running on the phone:

```
┌──────────────────────┐
│        420HD         │
│   Firmware Version   │
│    2.0.0_build_15    │
│                 Back │
└──────────────────────┘
```

Part X

Diagnostics and Troubleshooting

Reader's Notes

39   Testing Phone Hardware

The 310HD, 320HD and 420HD IP Phones Built-in Tests (BITs) are described below.

39.1   310HD IP Phone BIT

The 310HD IP Phone provides a built-in test for verifying its operational integrity. These tests can be performed before deployment and in cases of troubleshooting. These tests are all performed in one continuous sequence, where each test is followed by another consecutively, in the order listed below:

- Keypad and off-hook/on-hook test
- LED test
- Handset microphone (recording/speaking) and handset receiver (playing/listening) test
- Headset microphone (recording/speaking) and headset headphone/receiver (playing/listening) test
- Speaker microphone (recording/speaking) and speaker receiver (playing/listening) test
- MAC address and serial number verification

39.1.1   Test Preparation

Before you can start the built-in test, you need to cable the phone as follows:

1. Connect the phone's LAN port to a switch, using a LAN cable.
2. Ensure that the DHCP server is functioning.
3. Connect a headset to the phone.
4. Power on the phone and wait until initialization is complete.
5. From this stage onwards, follow the procedures described in the subsequent sections and in consecutive order. In other words, continue with the procedure described in Section 39.1.2 on page 236.

39.1.2   Keypad Test

The Keypad test checks the responsiveness and correct functioning of the keys on the phone's keypad.

➢ **To test the keypad:**

1. Using the keypad, dial the number "0123456789" and then press the star ("*") key; the phone's LCD screen displays the following:

Figure 39-1: Testing Keypad
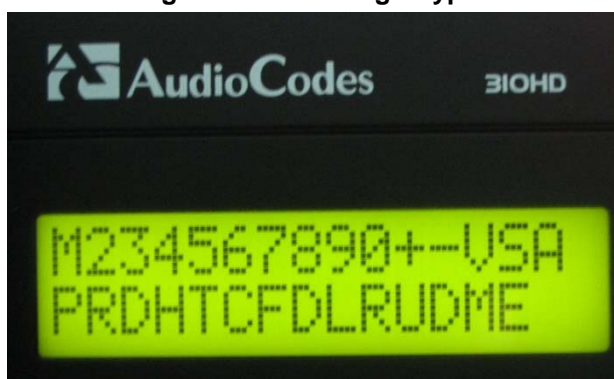
2. Press all keys except the keys 0-9, *, and #; for every key pressed, its corresponding character displayed on the LCD disappears.

Figure 39-2: Testing Keypad – Characters Disappear
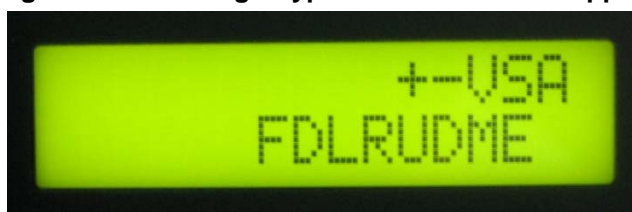
3. Continue with the LED test in Section 39.1.3 on page 237.

39.1.3 LED Test

Upon the successful completion of the Keypad test (in the previous section), the LCD screen displays the message "All LEDs are on. Press #" and the phone's single LED lights up red, as shown in the figure below:

Figure 39-3: Successful Completion of Keypad Test
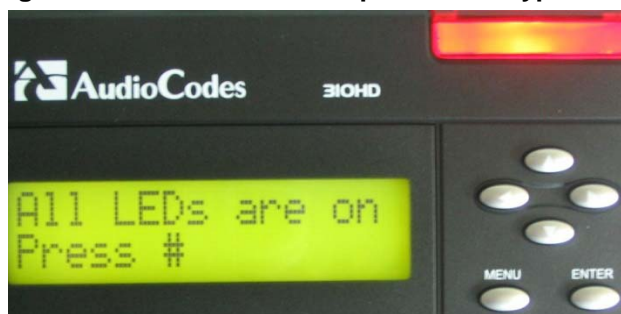
■   Continue with Handset test in Section .

39.1.4 Handset Test

Upon successful completion of the LED test (in the previous section), perform the Handset test. This test verifies the correct functioning of the handset, which includes the following:

■ Handset's microphone (transmitter) for speaking

■ Handset's receiver (speaker) for listening

➢ **To test the handset:**

1. Press the pound **(#)** key; the LCD screen displays the message "Handset test. Off hook to start".

Figure 39-4: Off hook Handset Test

2. Off hook the phone; the LCD screen displays the message "Recording".

Figure 39-5: Recording Test

3. Speak into the handset microphone; after about five seconds, the LCD screen displays the message "Playing".

Figure 39-6: Playing Test

4. The voice that was recorded when you spoke into the handset microphone is now played from the handset receiver.

5. Continue with the Headset test in Section 39.1.5 on page 239.

39.1.5 Headset Test

Upon successful completion of the Handset test (in the previous section), perform the Headset test. This test verifies the correct functioning of the headset (for hands-free operation), which includes the following:

■ Headset's microphone (transmitter) for speaking

■ Headset's headphone (receiver) for listening

➢ **To test the headset:**

    1. After about five seconds after your recorded voice is played in the Handset test (in the previous section), the LCD screen displays the message, "Headset test. Any key to start".

Figure 39-7: Headset Test

    2. Press any key; the LCD screen displays the "Recording" message.

Figure 39-8: Headset Recording Test

    3. Speak into the headset's microphone; after about five seconds, the LCD screen displays "Playing" and the voice that was recorded when you spoke into the headset's microphone is now played from the headset's receiver.

Figure 39-9: Headset Playing Test

    4. Continue with the Speaker test in Section .
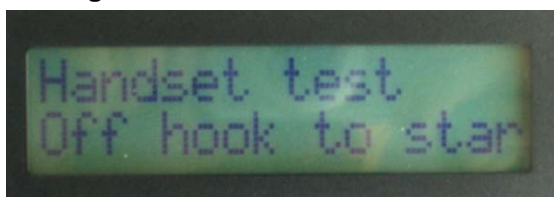
39.1.6 Speaker Test

Upon successful completion of the Headset test (in the previous section), perform the Speaker test. This test verifies the correct functioning of the speakers, which includes the following:

■ Speaker microphone (transmitter) for speaking (recording)

■ Speaker receiver for listening (playing)

➢ **To test the speaker:**

1. After about five seconds after your recorded voice is played in the Headset test (in the previous section), the LCD screen displays the message "Speaker/Mic test. Any key to start".

Figure 39-10: Speaker Test
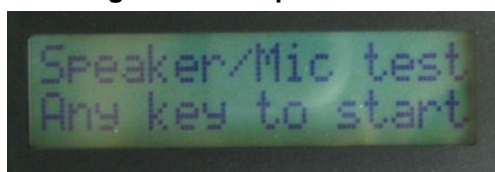
2. Press any key; the LCD screen displays the "Recording" message.

Figure 39-11: Speaker Recording Test
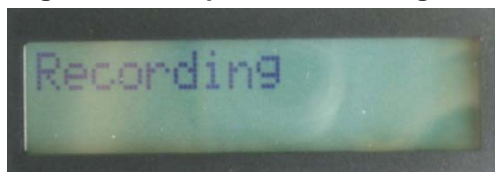
3. Speak into the phone's speaker microphone; after about five seconds, the LCD screen displays the message "Playing", and the voice that was recorded when you spoke into the speaker's microphone is now played from the speaker's receiver.

Figure 39-12: Speaker Playing Test

4. Continue with the MAC Address and Serial Number Verification test in Section 39.1.7 on page 241.

39.1.7   MAC Address and Serial Number Verification Test

The 310HD, 320HD and 420HD IP Phones MAC Address and Serial Number Verification Tests are described below.

39.1.7.1 MAC Address and Serial Number Verification Test

The MAC Address and Serial Number Verification test allows you to verify that the 310HD IP Phone's MAC address and serial number are correct.

➢ **To verify the MAC address and serial number:**

1.   After about five seconds after your recorded voice is played in the Speaker test (in the previous section), the LCD screen displays a MAC address and serial number:

Figure 39-13: MAC Address and Serial Number

2.   Check that the LAN MAC address and serial number are correct.

3.   Press any key to exit the phone's built-in test

39.2 Testing 320HD IP Phone BIT

The 320HD IP Phone provides a built-in test for verifying its operational integrity. This test can be performed before deployment and in cases of troubleshooting. The built-in test is comprised of numerous tests that are performed in one continuous sequence, where each test is followed by another consecutively, in the order listed below:

■ Keypad and off-hook/on-hook test

■ Green-color LEDs test

■ Red-color LEDs test

■ Handset microphone (recording/speaking) and handset receiver (playing/listening) test

■ Headset microphone (recording/speaking) and headset headphone/receiver (playing/listening) test

■ Speaker microphone (recording/speaking) and speaker receiver (playing/listening) test

■ MAC address and serial number verification

39.2.1 Test Preparation

Before you can start the built-in test, you need to cable the phone as follows:

1. Connect the phone's LAN port to a switch, using a LAN cable.

2. Ensure that the DHCP server is functioning.

3. Connect a headset to the phone.

4. Power on the phone and wait until initialization is complete.

5. From this stage onwards, follow the procedures described in the subsequent sections and in consecutive order. In other words, continue with the procedure described in Section 39.1.2 on page 236.

39.2.2 Keypad and Off-Hook/On-Hook Test

The Keypad and Off-Hook/On-Hook tests checks the responsiveness and correct functioning of the following:

■ All the keys on the phone's keypad

■ Handset when picked up (off-hook) and placed back on the receiver (on-hook)

➢ **To test the keypad and on-hook state:**

1. Using the keypad, dial the number "0123456789" and then press the star ("*") key; the phone's LCD screen displays a graphical display of the keypad, where each key has a corresponding indicator on the LCD screen.

Figure 39-14: Keypad Test
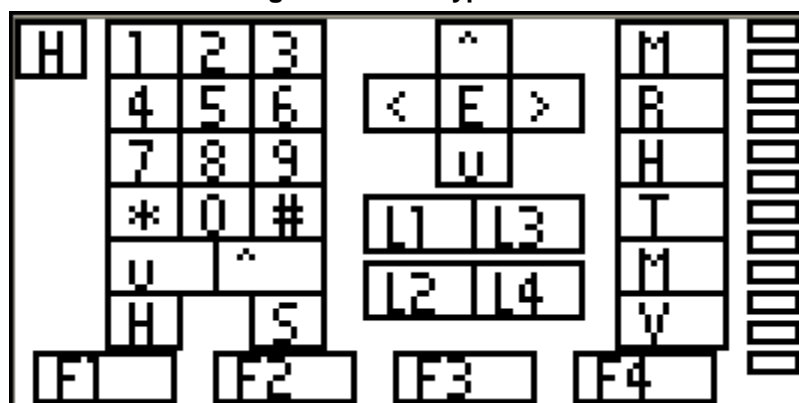
2. Off-hook the handset; the hook indicator ("H") on the LCD screen turns white on a black background.

Figure 39-15: Keypad Test – Off-Hook
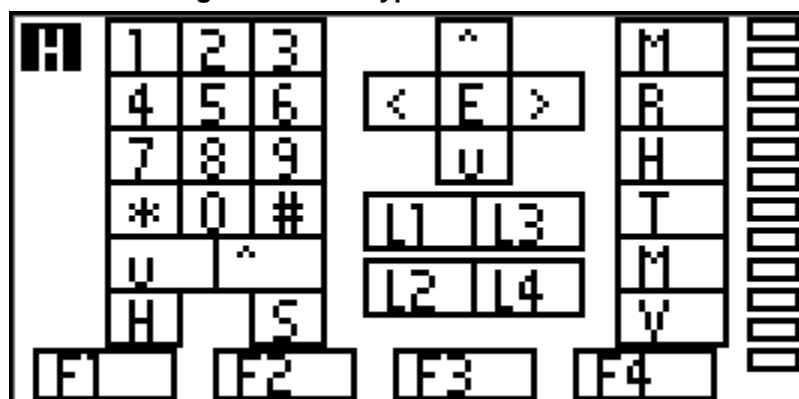
3. On-hook the handset; the hook indicator on the LCD screen turns white again.

4. Press each key on the phone's keypad; each key that is pressed turns its corresponding indicator on the LCD screen to the color black.

Figure 39-16: Keypad Test - Keys

5. Continue with the Green-color LEDs test in Section .
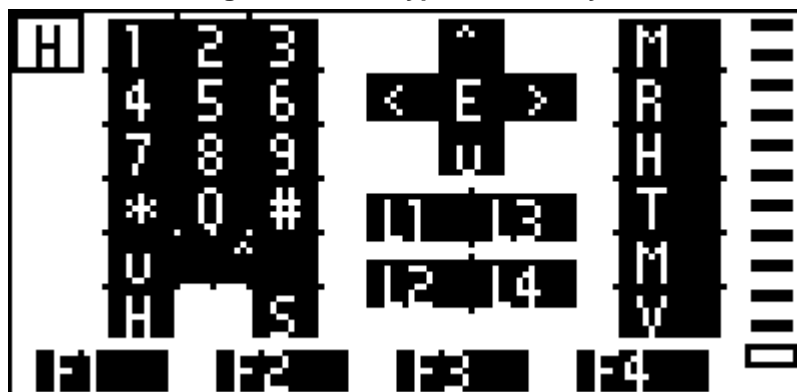
39.2.3   Green-Color LEDs Test

Upon the successful completion of the Keypad and On-Hook/Off-Hook test (in the previous section), the LCD screen displays the message "Green LEDs are on". Consequently, all LEDs light up green (except the VOICE MAIL, HEADSET, SPEAKER, and MUTE LEDs, which are red only), as shown in the figure below:

Figure 39-17: Green LEDs On

Continue with the Red-Color LEDs test in Section 39.2.4 on page 246.

39.2.4 Red-Color LEDs Test

Upon the completion of the Green-Color LEDs test (in the previous section), perform the Red-color LEDs test for verifying that the red light is functioning for the phones LEDs.

➤ **To test the LEDs for red-color lighting:**

1. Press any key; all the LEDs turn red, as shown in the figure below:

Figure 39-18: Red LEDs Test

2. Continue with the Handset test in Section 39.2.5 on page 247.

39.2.5   Handset Test

Upon successful completion of the Red-color LEDs test (in the previous section), perform the Handset test. This test verifies the correct functioning of the handset, which includes the following:

■   Handset's microphone (transmitter) for speaking

■   Handset's receiver (speaker) for listening

➢   **To test the handset:**

1.   Press any key; the LCD screen displays the message "Prepare to test handset. Off hook to start".

Figure 39-19: Handset Test


```
10.16.2.10
Handset Test
Off-hook phone
```

2.   Off hook the phone; the LCD screen displays the message "start recording".

Figure 39-20: Handset Test - Recording
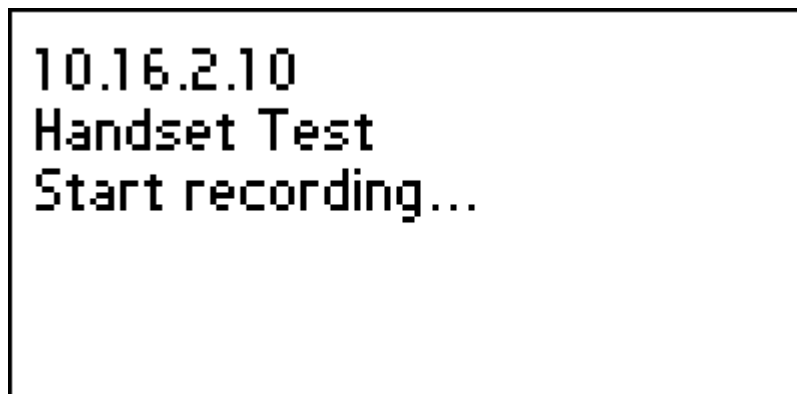

```
10.16.2.10
Handset Test
Start recording...
```

3. Speak into the handset microphone; after about five seconds, the LCD screen displays the message "start playing".

Figure 39-21: Handset Test- Playing

```
10.16.2.10
Handset Test
Start playing...
```
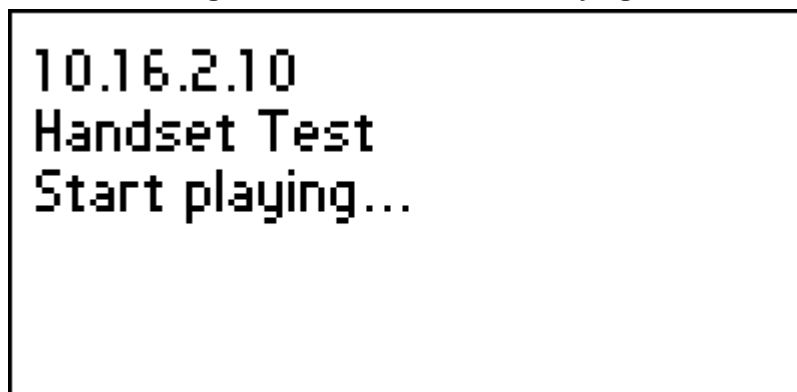
The voice message that was recorded when you spoke into the handset microphone is now played from the handset receiver.

4. Continue with the Headset test in Section 39.1.5 on page 239.

39.2.6 Headset Test

Upon successful completion of the Handset test (in the previous section), perform the Headset test. This test verifies the correct functioning of the headset (for hands-free operation), which includes the following:

■ Headset's microphone (transmitter) for speaking

■ Headset's headphone (receiver) for listening

➢ **To test the headset:**

1. After about five seconds after your recorded voice is played in the Handset test (in the previous section), the LCD screen displays the message "Prepare to test headset. Press any key to start".

Figure 39-22: Headset Test

```
10.16.2.10
Headset Test
Press any key
```
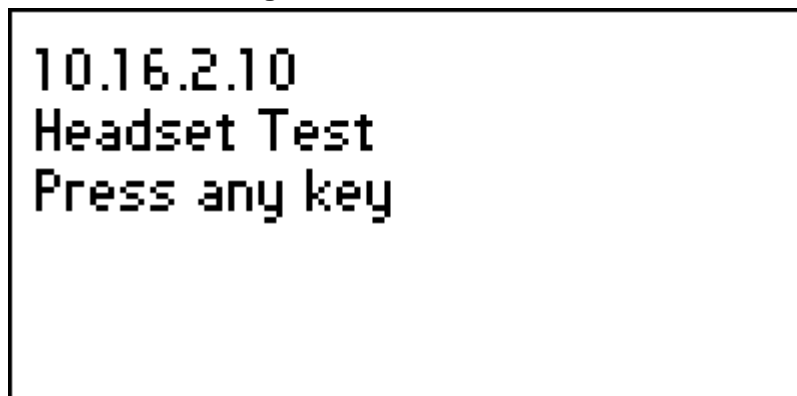
2. Press any key; the LCD screen displays the message "start recording".

Figure 39-23: Headset Test - Recording

```
10.16.2.10
Headset Test
Start recording...
```
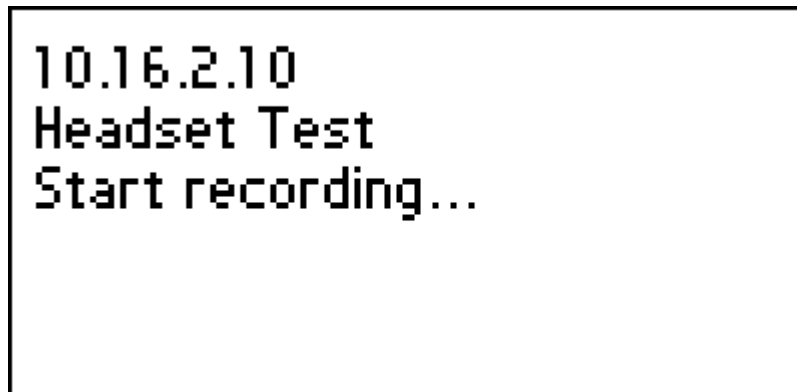
3. Speak into the headset's microphone; after about five seconds, the LCD screen displays "start playing" and the voice that was recorded when you spoke into the headset's microphone is now played from the headset's receiver.

Figure 39-24: Headset Test - Playing

```
10.16.2.10
Headset Test
Start playing...
```
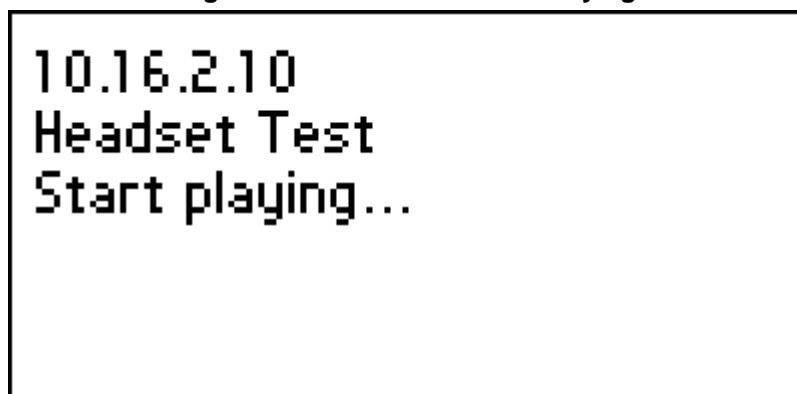
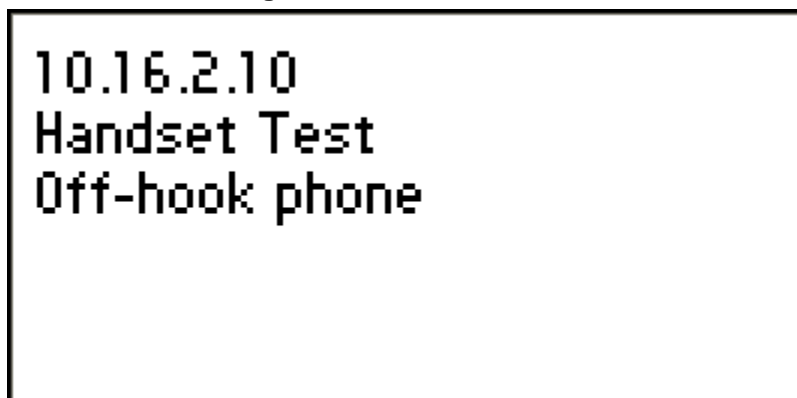**4.** Continue with the Speaker test in Section .

39.2.7 Speaker Test

Upon successful completion of the Headset test (in the previous section), perform the Speaker test. This test verifies the correct functioning of the speakers, which includes the following:

■ Speaker microphone (transmitter) for speaking (recording)

■ Speaker receiver for listening (playing)

➢ **To test the speaker:**

1. After about five seconds after your recorded voice is played in the Headset test (in the previous section), the LCD screen displays the message "Speaker/Mic Test. Press any key".

Figure 39-25: Speaker/Mic Test
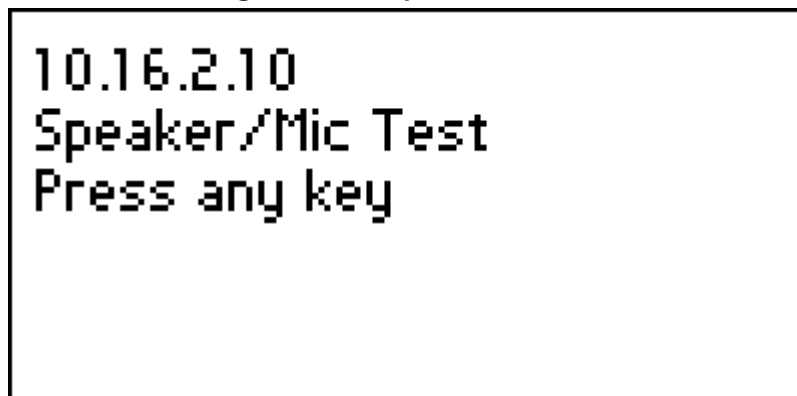
2. Press any key; the LCD screen displays the message "Start recording".

Figure 39-26: Speaker/Mic Test– Recording
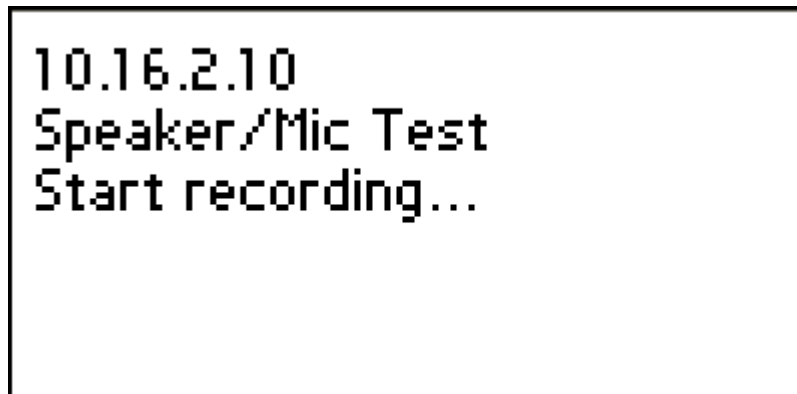
3. Speak into the phone's speaker microphone; after about five seconds, the LCD screen displays the message "playing", and the voice that was recorded when you spoke into the speaker's microphone is now played from the speaker's receiver.

Figure 39-27: Speaker/Mic Test – Playing
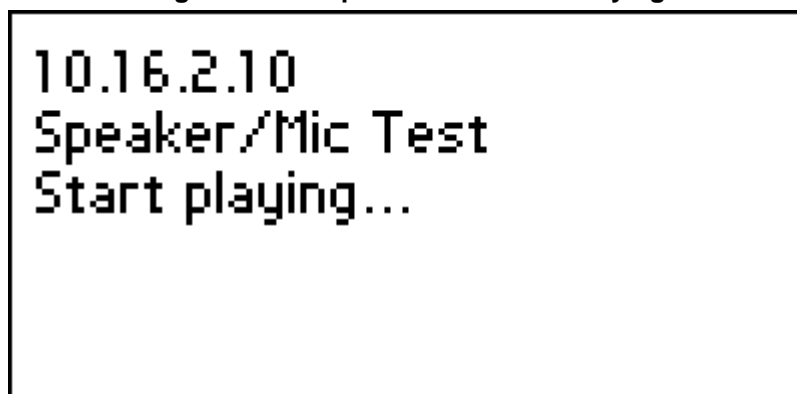
```
10.16.2.10
Speaker/Mic Test
Start playing...
```

4. Continue with the MAC Address and Serial Number Verification test in Section .
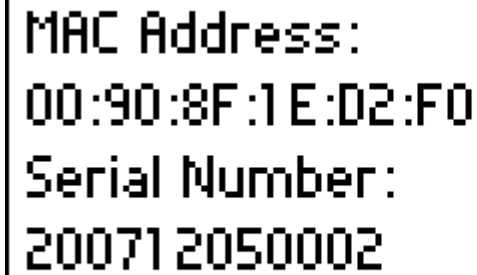
39.2.8 MAC Address and Serial Number Verification Test

The MAC Address and Serial Number Verification test allows you to verify that the phone's MAC address and serial number are correct.

➢ **To verify the MAC Address and Serial Number:**

1. After about five seconds after your recorded voice is played in the Speaker test (in the previous section), the LCD screen displays a MAC address and serial number:

Figure 39-28: MAC Address and Serial Number Verification Test

```
MAC Address:
00:90:8F:1E:D2:F0
Serial Number:
200712050002
```

2. Check that the LAN MAC address and serial number are correct.

3. Press any key to exit the phone's built-in test.

39.3 Testing 420HD IP Phone BIT

The BIT for the 420HD IP Phone is identical to that of the 320HD IP Phone (see Section 39.2 on page 242).

Reader's Notes

40   Recovering Firmware

If the phone is powered off for some reason during the firmware upgrade process, the phone becomes unusable.

> ➢ **To recover the phone firmware:**

1. Ensure that your DHCP server supports Options 66 (TFTP server address) and 67 (firmware file), and that these are configurable.

2. Before connecting the phone, verify that the TFTP server is running and the firmware file for recovery is located in the correct location.

3. Connect your phone to the IP network, and then connect the phone to the power outlet;

    a. The phone sends a TFTP request to the IP address indicated in the DHCP Option 66 field to retrieve the firmware file indicated in the DHCP Option 67 field.

    b. The phone, in the DHCP Discover message sends its model name in the DHCP Option 77 field. The DHCP server, according to the phone model, sets the appropriate firmware file name in the DHCP Option 67 field sent to the phone (e.g., 310HD_1.4.1_build_32.img).

    c. The phone then upgrades to the recovery firmware.

    d. After the firmware upgrade process completes, the phone boots up successfully.

Reader's Notes

41   System Logging (Syslog)

System logging can be configured using the Web or Configuration File, as described below.

➤ **To configure system logging:**

■ **Using the Web:**

1.   Access the 'System logging' page (**Status & Diagnostics** tab > **Diagnostics** menu > **Logging**).

Figure 41-1: System Logging Web Fields

2.   Configure system logging according to the parameters in the table below, and then click **Submit**.

■ **Using the Configuration File:**

Table 41-1: Syslog Parameters

Parameter	Description
Note: To add a value to these parameters, enter **system/** followed by the parameter name, equal sign and then the value (e.g. system/syslog/mode=UDP).	
Activate **[system/watchdog/enabled]**	Enables the system watchdog. Possible values are: • **Disable** = No Syslog. • **Network** = Syslog is sent to the Syslog server. (Recommended). • **Console** = Syslog is sent to the phone console. (You need to connect a serial cable to view the logs. This causes delays in phone operation). • **Both** = Syslog sends to the Syslog server AND the console. **Note:** It is recommended to leave this parameter at its default value.

Parameter	Description
Server IP Address or Host Name **[system/syslog/server_address]**	The IP address (in dotted-decimal notation) of the computer you are using to run the Syslog server (e.g. Wireshark). The Syslog server is an application designed to collect the logs and error messages generated by the phone. The default IP address is 0.0.0.0. **Note:** This parameter is applicable when Activate is set to "Network" or "Both".
Server Port **[system/syslog/server_port]**	Defines the UDP port of the Syslog server. The valid range is 0 to 65,535. The default port is 514. **Note:** This parameter is applicable when Activate is set to "Network" or "Both".
Note: The following Severity level options are applicable for the fields below: • None • Emergency • Error • Waiting • Notice • Info • Debug	
VoIP Application	Defines multi-layer VoIP application.
SIP Call Control	Defines MTR layer Radvision.
SIP Stack	Defines SIP Stack Radvision.
Control Center	Responsible for Networking and running other processes.
LCD Display	Defines LCD Display.
CGI	Defines services for the Web server.
Web Server	Defines the phone Web server.
Watchdog	Responsible for keeping other processes running.
802.1X	Defines the security protocol.

42   Phone User Interface Error Messages

The following Phone User Interface error messages may appear on the IP Phone.

Table 42-1: Phone User Interface Error Messages

Message	Description
LAN Link failure	The LAN link is disconnected.
Registration failure	Received error or no response from the SIP proxy

Notes:

- With both errors, the "ringer" LED remains red until the error is fixed.
- While the error message is displayed, the user can`t dial or initiate a call.

Reader's Notes

43   Media Debug Information

Recording parameters allows you to debug the voice activity of the phone, using the Web or Configuration File, as described below.

➢ **To define media debug information:**

■ **Using the Web:**

1. Access the 'Recording' page (**Status & Diagnostics** tab > **Diagnostics** menu > **Recording**).

Figure 43-1: Recording Web Fields

2. Configure Media Debug Recording according to the parameters in the table below, and then click **Submit**.

■ **Using the Configuration File:**

Table 43-1: Packet Recording Parameters

Parameter	Description
Enable DSP Recording **[voip/packet_recording/enabled]**	Activates the packet recording mechanism. ▪ **[0]** Disable (default) ▪ **[1]** Enable
Remote IP Address or Host Name **[voip/packet_recording/remote_ip]**	The IP address (in dotted-decimal notation) of the remote computer to which the recorded packets are sent. The recorded packets should be captured by a network sniffer (such as Wireshark). The default value is 0.0.0.0.
Remote Port **[voip/packet_recording/remote_port]**	Defines the UDP port of the remote computer to which the recorded packets are sent. The valid range is 1024 to 65535. The default value is 50000.
Enable RTP Recording **[voip/packet_recording/rtp_recording/enabled]**	Activates the DSP RTP recording. ▪ **[0]** Disable (default) ▪ **[1]** Enable

Parameter	Description
Enable EC Debug Recording **[voip/packet_recording/ec_debug_recording/enabled]**	Activates the Echo Canceller Debug recording. ▪ **[0]** Disable (default) ▪ **[1]** Enable
Enable Network Recording **[voip/packet_recording/network_recording/enabled]**	Activates the DSP network (TDM Out) recording. ▪ **[0]** Disable (default) ▪ **[1]** Enable
Enable TDM Recording **[voip/packet_recording/tdm_recording/enabled]**	Activates the DSP TDM (TDM In) recording. ▪ **[0]** Disable (default) ▪ **[1]** Enable

44   Port Mirroring
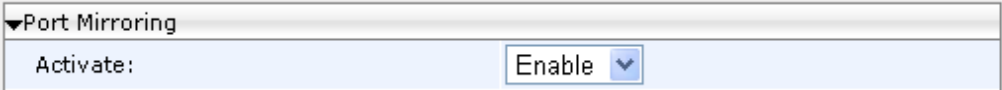
Port mirroring can be configured using the Web or Configuration File, as described below.

➢ **To configure port mirroring:**

■ **Using the Web:**

1. Access the 'Recording' page (**Configuration** tab > **Network Connections** menu > **Network Settings**).

Figure 44-1: Port Mirroring

2. Configure port mirroring according to the parameters in the table below, and then click **Submit**.

■ **Using the Configuration File:**

Table 44-1: Port Mirroring Parameters

Parameter	Description
Activate **[network/pc_port_mirroring/enabled]**	Enables port mirroring. ▪ **[0]** Disable (default) **-** The LAN/PC Network interfaces operate in SWITCH mode. ▪ **[1]** Enable **-** The LAN/PC Network interfaces operate in HUB mode. The network traffic on the LAN port is reflected in the PC port.

Reader's Notes

Part XI

Appendices

Reader's Notes

A   Server-Specific Configuration

> **Note:** This appendix is only applicable to the 320HD IP Phone.

A.1   Lync (SPS only)

Lync can be configured using the Configuration File, as described below.

Table A-1: Busy Lamp Field Parameter

Parameter	Description
/voip/services/busy_lamp_field/color_settings	Relevant for presence feature. Valid values: **[OPTION_1]** = BLF refers the presence state of remote parties. **[OPTION_2]** = BLF refers the call state of remote parties (default).

A.2   BroadWorks

The configuration of the BLF feature is unique when the selected application server is BroadWorks™.

➤ **To configure BLF for BroadWorks:**

1. Access the Services page (**Configuration** tab > **Voice Over IP** menu > **Services**). The figure's callouts below correspond to the steps in this procedure:

Figure A-1: BLF Configuration for BroadWorks Web Fields

2. From the 'Application Server Type' drop-down list, select **BSF**.

3. In the **BLF Support** group, do the following:

    a. From the 'Activate' drop-down list (*voip/services/busy_lamp_field/enabled* parameter), select **Enable**.

    b. In the 'BLF Subscription Period' field (*voip/services/busy_lamp_field/subscription_period* parameter), enter the interval between BLF and SIP SUBSCRIBE messages.

    c. In the 'User Resource List' field (*voip/services/busy_lamp_field/uri* parameter), enter the resource list URI to which the phone can subscribe to in order to get the BLF information from the application server.

    d. Define the Application Server Address:

        ♦ **Same address as SIP Registrar:** From the 'Use Registrar as Application Server Address' (*voip/services/busy_lamp_field/application_server/use_registrar* parameter) drop-down list, select **Enable**. The Registrar's address is used as the application server's address, defined by the parameter *voip/signalling/sip/sip_registrar/addr* (refer to Section 17.2 on page 93).

        ♦ **Unique address:** From the 'Use Registrar as Application Server Address' drop-down list, select "Disable", and then in the "Application Server Address or Domain Name" field (*voip/services/busy_lamp_field/application_server/addr* parameter), enter the IP address or domain name of the application server.

4. Click **Submit**.

5. Define speed dial keys with the BLF feature (see Section 26 on page 175).
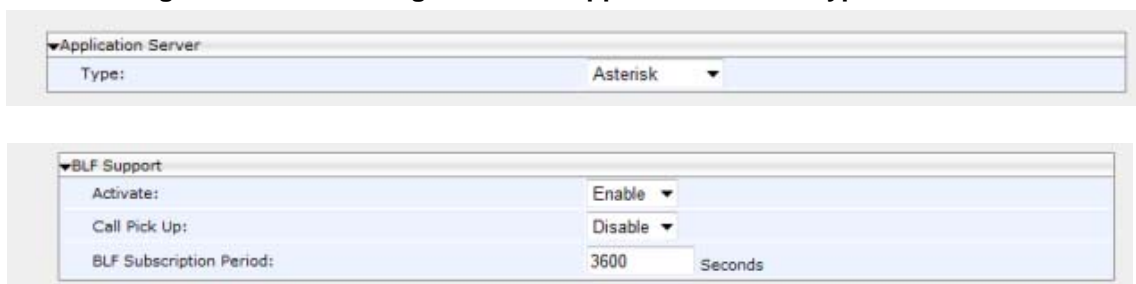
A.3 Configuring BLF for Asterisk, Coral and Metaswitch

The configuration of the BLF feature is unique when the selected application server is **Asterisk**, **Coral**, or **Metaswitch**.

➢ **To configure BLF for Asterisk application server:**

1. Access the Services page (**Configuration** tab > **Voice Over IP** menu > **Services**). The figure's callouts below correspond to the steps in this procedure:

Figure A-2: BLF Configuration for Application Server Type - Asterisk

2. From the 'Application Server Type' drop-down list, select one of the following:
   - Asterisk
   - Coral
   - Metaswitch
3. In the **BLF Support** group, configure the following:
   a. From the 'Activate' drop-down list (*voip/services/busy_lamp_field/enabled* parameter), select **Enable**.
   b. (Optional) In the 'BLF Subscription Period' field (*voip/services/busy_lamp_field/subscription_period* parameter), enter the interval between BLF and SIP SUBSCRIBE messages.

⚠️ **Note:** The application server's address is the same as the SIP Registrar

4. Click **Submit**.
5. Define speed dial keys with the BLF feature (see Section 26 on page 175).

B   Typical Setup Scenario Example

In the sample scenario below, the IT manager plans to deploy out-of-the-box IP phones in the office. AudioCodes' configuration tool is used to prepare a configuration file per phone (based on MAC addresses). The configuration files are downloaded from the office's HTTP server. DHCP is used to point the phone to the HTTP server.

➢ **To prepare the template configuration file:**

1. Connect an out-of-the box IP Phone to a regular LAN and wait for it to boot up.
2. Check the phone's IP address using the User Interface (**Menu** > **Status** > **Network Status**).
3. Connect to the phone's embedded web server using **http://<phone IP address>.**
4. Make sure the phone is running the latest firmware version (shown on the home page). If not, obtain a new firmware file and download it using **Management** > **Manual Update** > **Firmware Upgrade**.
5. If the phone's configuration has been modified in the past, restore the default configuration using **Management** > **Administration** > **Restore Defaults**.
6. Access **Management** > **Manual Update** > **Configuration File** and save a copy of the original configuration file.
7. Make the required configuration changes (e.g. VoIP parameters) via Web.
8. Make sure the IP Phone functions properly in your network.
9. Access **Management** > **Manual Update** > **Configuration file** and save the modified configuration file.
10. Compare the two configuration files and create a file containing only the modified lines.

➢ **To create MAC-specific files using AudioCodes' configuration tool:**

1. Edit the template configuration file and replace each parameter value that should be different per user (e.g. the line ID) with a tag (e.g. [id]).
2. Prepare a *.csv* file with a list of the MAC addresses of the phones you plan to deploy and the parameters values each user.
3. Run the configuration too to generate the configurations files (one per phone).
4. Save the configuration files on the HTTP server.

➢ **To prepare the DHCP server:**

• Configure OPTION 160 on the DHCP with the URL of the configuration files on the HTTP server. Use the string <MAC> to indicate the phone's MAC address, for example: **http://192.168.2.1/:310HD_<MAC>_conf.cfg**.

➢ **To verify the setup:**

1. Connect one of the IP Phones for deployment to the network.
2. Follow the status displayed on the LCD. Make sure the phone received an IP address and is upgrading the configuration.
3. The phone reboots with the new configuration.
4. Make sure all functionality works well (e.g. can make VoIP calls).

Reader's Notes

C   SIP Support (RFC, Headers)

The following is a list of supported SIP RFCs and Methods that you can use to create for the IP Phone.

Table C-1: Supported IETF RFC's

RFC Number	RFC Title
RFC 2327	SDP
RFC 2617	HTTP Authentication: Basic and Digest Access Authentication
RFC 2782	A DNS RR for specifying the location of services
RFC 2833	Telephone event
RFC 3261	SIP
RFC 3262	Reliability of Provisional Responses in SIP
RFC 3263	Locating SIP Servers
RFC 3264	Offer/Answer Model
RFC 3265	(SIP)-Specific Event Notification
RFC 3310	Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)
RFC 3311 (Partially Supported)	UPDATE Method
RFC 3326 (Partially Supported)	Reason header
RFC 3389	RTP Payload for Comfort Noise
RFC 3515	Refer Method
RFC 3605	RTCP attribute in SDP
RFC 3611	RTP Control Protocol Extended Reports (RTCP XR)
RFC 3665	SIP Basic Call Flow Examples
RFC 3711	The Secure Real-time Transport Protocol (SRTP)
RFC 3725	Third Party Call Control
RFC 3842	MWI
RFC 3891	"Replaces" Header
RFC 3892 (Sections 2.1-2.3 and 3 are supported)	The SIP Referred-By Mechanism
RFC 3960 (Partially Supported)	Early Media and Ringing Tone Generation in SIP (partial compliance)
RFC 3966	The tel URI for Telephone Numbers
RFC 4028 (Partially Supported)	Session Timers in the Session Initiation Protocol
RFC 4240	Basic Network Media Services with SIP - NetAnn
draft-ietf-sip-privacy-04.txt (Partially Supported)	SIP Extensions for Network-Asserted Caller Identity using Remote-Party-ID header
draft-ietf-sipping-cc-transfer-05	Call Transfer

RFC Number	RFC Title
draft-ietf-sipping-realtimefax-01	SIP Support for Real-time Fax: Call Flow Examples
draft-choudhuri-sip-info-digit-00	SIP INFO method for DTMF digit transport and collection
draft-mahy-sipping-signaled-digits-01	Signaled Telephony Events in the Session Initiation Protocol

Note: The following SIP features are not supported:

- Preconditions (RFC 3312)
- SDP - Simple Capability Declaration (RFC 3407)
- S/MIME
- Outbound, Managing Client-Initiated Connections (RFC 5626)
- SNMP SIP MIB (RFC 4780)
- SIP Compression – RFC 5049 (SigComp)
- ICE (RFC 5245)
- Connected Identity (RFC 4474)

C.1   SIP Compliance Tables

The SIP device complies with RFC 3261, as shown in the following subsections.

C.1.1   SIP Methods

The device supports the following SIP Methods:

Table C-2: Supported SIP Methods

Method	Supported	Comments
INVITE	Yes	
ACK	Yes	
BYE	Yes	
CANCEL	Yes	
REGISTER	Yes	Send only
REFER	Yes	Inside and outside of a dialog
NOTIFY	Yes	
INFO	Yes	
OPTIONS	Yes	
PRACK	Yes	
PUBLISH	Yes	Send only
SUBSCRIBE	Yes	

C.1.2   SIP Headers

The device supports the following SIP Headers:

Table C-3: Supported SIP Headers

Header Field	Supported
Accept	Yes
Alert-Info	Yes
Allow	Yes
Authorization	Yes
Call-ID	Yes
Call-Info	Yes
Contact	Yes
Content-Length	Yes
Content-Type	Yes
Cseq	Yes
Date	Yes
Diversion	Yes
Encryption	No
Expires	Yes
Fax	Yes
From	Yes
History-Info	Yes
Join	Yes
Max-Forwards	Yes
MIN-SE	Yes
P-Asserted-Identity	Yes
P-Preferred-Identity	Yes
Proxy- Authenticate	Yes
Proxy- Authorization	Yes
Prack	Yes
Record- Route	Yes
Refer-To	Yes
Referred-By	Yes
Replaces	Yes
Remote-Party-ID	Yes
Retry-After	Yes
Route	Yes

Header Field	Supported
Session-Expires	Yes
Supported	Yes
Timestamp	Yes
To	Yes
Unsupported	Yes
User- Agent	Yes
Via	Yes
Voicemail	Yes
Warning	Yes
WWW- Authenticate	Yes

Reader's Notes

D   IP Phone Specifications

The 310HD, 320HD and 420HD IP Phones specifications are listed in the table below.

Table D-1: 310HD, 320HD and 420HD IP Phone Specifications

Feature	Details
VoIP Signaling Protocols	▪ SIP: RFC 3261, RFC 2327 (SDP)
Data Protocols	▪ IPv4, TCP, UDP, ICMP, ARP, DNS and DNS SRV for SIP Signaling ▪ SIP over TLS (SIPS) ▪ 802.1p/Q for Traffic Priority and QoS ▪ VLAN Discovery Mechanism (CDP, LLDP) ▪ ToS (Type of Service) field, indicating desired QoS DHCP Client ▪ NTP Client
Media Processing	▪ Voice Coders: G.711, G.723.1, G.729A/B, G.722, RTA. ▪ Acoustic Echo Cancelation: G.168-2004 compliant, 64-msec tail length ▪ Adaptive Jitter Buffer 300 msec ▪ Voice Activity Detection ▪ Comfort Noise Generation ▪ Packet Lost Concealment ▪ RTP/RTCP Packetization (RFC 3550, RFC 3551), SRTP (RFC 3711) ▪ DTMF Relay (RFC 2833)
Telephony Features	▪ Call Hold / Un-Hold ▪ Call Transfer ▪ 3-Way Conferencing (with local mixing) ▪ Redial ▪ Caller ID Notification ▪ Call Waiting Indication ▪ Message Waiting Indication (including MWI LED) ▪ Local and Corporate Directories ▪ Automatic On-hook Dialing ▪ Automatic Answering (Alert-Info header and "talk" event) ▪ CWRR (Call Waiting Reminder Ring) ▪ Secondary Dial Tone ▪ Call Logs: Missed/Received Calls and Dialed Numbers ▪ Speed Dial (Including BLF support for Asterisk and BroadWorks^{TM}) ▪ Dial Plan ▪ URL Dialing ▪ Advice of Charge (AOC) ▪ Call Forward (Unconditional, Busy, No Answer) ▪ Redundant SIP Proxy Mechanism ▪ Remote Conferencing (RFC 4240) ▪ Multiple Lines for 320HD (currently supports up to 4 lines)

Feature	Details
Configuration/ Management	▪ TR-069 for remote configuration and management ▪ LCD Display User Interface Language Support (Various Languages) ▪ Web-based Management (HTTP/HTTPS) ▪ Auto-Provisioning (via TFTP, FTP, HTTP, and HTTPS) for firmware and configuration file upgrade ▪ DHCP options (66, 67, and 160) for Auto-provisioning ▪ DHCP options (12, 60, and 77) for device information ▪ Private labeling mechanism ▪ Configuration file encryption (entire file and individual parameters)
Debugging Tools	▪ Syslog mechanism ▪ DSP recording ▪ Port mirroring ▪ VoIP Status Web page

310HD Hardware	▪ **LCD screen:** 2 * 16 characters
	▪ **Connectors interfaces:**
	  ✓ 2 x RJ-45 ports (10/100BaseT Ethernet) for WAN and LAN
	  ✓ RJ-9 port (jack) for Headset
	  ✓ RJ-9 port (jack) for Handset
	▪ **Mounting:**
	  ✓ Wall mounting
	  ✓ Adjustable angle tilt for desktop mounting
	▪ **Power:**
	  ✓ DC jack adapter 12V
	  ✓ Power supply AC 100 ~ 240V
	  ✓ PoE: IEEE802.3af (optional)
	▪ **Keys:**
	  ✓ 10 x speed dial keys
	  ✓ VOICE MAIL message hotkey
	  ✓ 4-way navigation keys with ENTER Key
	  ✓ MENU
	  ✓ DIRECTORY
	  ✓ REDIAL
	  ✓ HOLD
	  ✓ MUTE
	  ✓ TRANSFER
	  ✓ CONFERENCE
	  ✓ FORWARD
	  ✓ DND
	  ✓ VOLUME control key
	  ✓ HEADSET
	  ✓ SPEAKER

Feature	Details

320HD Hardware	▪ **LCD screen:** Graphic LCD (132*64) mono
	▪ **Connectors interfaces:**
	  ✔ 2 x RJ-45 ports (10/100BaseT Ethernet) for WAN and LAN
	  ✔ RJ-9 port (jack) for Headset
	  ✔ RJ-9 port (jack) for Handset
	▪ **Mounting:**
	  ✔ Wall mounting
	  ✔ Adjustable angle tilt for desktop mounting
	▪ **Power:**
	  ✔ DC jack adapter 12V
	  ✔ Power supply AC 100 ~ 240V
	  ✔ PoE: IEEE802.3af (optional)
	▪ **Keys:**
	  ✔ 12 x speed dial keys
	  ✔ Line 1 ~ 2 (LED)
	  ✔ 4 x softkeys
	  ✔ VOICE MAIL message hotkey with LED indicator
	  ✔ 4-way navigation keys with ENTER Key
	  ✔ MENU
	  ✔ REDIAL
	  ✔ HOLD
	  ✔ MUTE (LED)
	  ✔ TRANSFER
	  ✔ VOLUME control key
	  ✔ HEADSET
	  ✔ SPEAKER

420HD Hardware	▪ **LCD screen:** Graphic LCD (132*64) mono
	▪ **Connectors interfaces:**
	  ✔ 2 x RJ-45 ports (10/100BaseT Ethernet) for WAN and LAN
	  ✔ RJ-9 port (jack) for Headset
	  ✔ RJ-9 port (jack) for Handset
	▪ **Mounting:**
	  ✔ Wall mounting
	  ✔ Adjustable angle tilt for desktop mounting
	▪ **Power:**
	  ✔ DC jack adapter 12V
	  ✔ Power supply AC 100 ~ 240V
	  ✔ PoE: IEEE802.3af (optional)
	▪ **Keys:**
	  ✔ 4 x softkeys
	  ✔ VOICE MAIL message hotkey
	  ✔ 4-way navigation keys with ENTER Key
	  ✔ MENU
	  ✔ REDIAL
	  ✔ HOLD
	  ✔ MUTE
	  ✔ TRANSFER
	  ✔ VOLUME control key
	  ✔ HEADSET
	  ✔ SPEAKER

Feature	Details
Headset Compatibility	▪ GN.com 2100 – both single and dual ▪ Jabra BIZ 2400 – both single and dual ▪ GN.com 9350 ▪ Plantronics H261N ▪ Plantronics H251N

Reader's Notes

AudioCodes Series of High Definition IP Phones

HD VoIP

Administrator's Manual

310HD / 320HD / 420HD IP Phones

Version 2.0.0